


Springer Optimization and Its Applications 205

Konstantinos P. Balomenos  
Antonios Fytopoulos  
Panos M. Pardalos *Editors*

# Handbook for Management of Threats

Security and Defense, Resilience and  
Optimal Strategies

 Springer

# Springer Optimization and Its Applications

Volume 205

## Series Editors

Panos M. Pardalos , *University of Florida*

My T. Thai , *University of Florida*

## Honorary Editor

Ding-Zhu Du, *University of Texas at Dallas*

## Advisory Editors

Roman V. Belavkin, *Middlesex University*

John R. Birge, *University of Chicago*

Sergiy Butenko, *Texas A&M University*

Vipin Kumar, *University of Minnesota*

Anna Nagurney, *University of Massachusetts Amherst*

Jun Pei, *Hefei University of Technology*

Oleg Prokopyev, *University of Pittsburgh*

Steffen Rebennack, *Karlsruhe Institute of Technology*

Mauricio Resende, *Amazon*

Tamás Terlaky, *Lehigh University*

Van Vu, *Yale University*

Michael N. Vrahatis, *University of Patras*

Guoliang Xue, *Arizona State University*

Yinyu Ye, *Stanford University*

## **Aims and Scope**

Optimization has continued to expand in all directions at an astonishing rate. New algorithmic and theoretical techniques are continually developing and the diffusion into other disciplines is proceeding at a rapid pace, with a spot light on machine learning, artificial intelligence, and quantum computing. Our knowledge of all aspects of the field has grown even more profound. At the same time, one of the most striking trends in optimization is the constantly increasing emphasis on the interdisciplinary nature of the field. Optimization has been a basic tool in areas not limited to applied mathematics, engineering, medicine, economics, computer science, operations research, and other sciences.

The series **Springer Optimization and Its Applications (SOIA)** aims to publish state-of-the-art expository works (monographs, contributed volumes, textbooks, handbooks) that focus on theory, methods, and applications of optimization. Topics covered include, but are not limited to, nonlinear optimization, combinatorial optimization, continuous optimization, stochastic optimization, Bayesian optimization, optimal control, discrete optimization, multi-objective optimization, and more. New to the series portfolio include Works at the intersection of optimization and machine learning, artificial intelligence, and quantum computing.

*Volumes from this series are indexed by Web of Science, zbMATH, Mathematical Reviews, and SCOPUS.*

Konstantinos P. Balomenos •  
Antonios Fytopoulos • Panos M. Pardalos  
Editors

# Handbook for Management of Threats

Security and Defense, Resilience  
and Optimal Strategies


 Springer



*Editors*

Konstantinos P. Balomenos  
Director General of General Directorate of  
National Defence Policy  
International Relations – Hellenic Ministry  
of National Defense  
Athens, Greece

Antonios Fytopoulos  
Department of Chemical Engineering  
KU Leuven  
Leuven, Belgium  
School of Chemical Engineering NTUA  
Athens, Greece

Panos M. Pardalos   
Department of Industrial and Systems  
Engineering  
University of Florida  
Gainesville, FL, USA

ISSN 1931-6828                      ISSN 1931-6836 (electronic)  
Springer Optimization and Its Applications  
ISBN 978-3-031-39541-3              ISBN 978-3-031-39542-0 (eBook)  
<https://doi.org/10.1007/978-3-031-39542-0>

Mathematics Subject Classification: 49M99, 93-10

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

This work is subject to copyright. All rights are solely and exclusively licensed 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

Paper in this product is recyclable.

“Σα βγεις στον πηγαιμό για την  
Ιθάκη,  
να εύχεται νάναι μακρύς ο δρόμος,  
γεμάτος περιπέτειες, γεμάτος  
γνώσεις.  
...”

**Ιθάκη**  
**Κ.Π. Καβάφης**

# Preface

Over the last 20 years, humanity has faced unprecedented challenges and threats, such as several terrorist attacks, the international financial crisis, the COVID-19 pandemic, competition for energy, regional conflicts in the periphery of Europe and all over the world, climate change, and disruptive technologies, to name just a few.

These examples highlight the enhanced interaction and connectivity among the fundamental elements of the current globalized world. Companies, countries, and people interact in a complex way on common grounds like the global monetary system and international laws, using technological tools to enhance this interconnectivity even more and leading to an interdependent world. Modern people can gain access to an abundance of information and resources, but at the same time can be much more affected by emerging threats; it is certain that the expansion of networks will lead to the increasing influence due to potential disasters. The goal of this handbook is to identify the most probable threats that could affect humanity in recent and following years, to evaluate their effects on people, and to propose ways to mitigate these effects.

The book starts with chapter “[Future Threats](#)”, an introductory chapter that summarizes potential future threats that could harm humanity and highlights the necessity for resilience, which is the ability to restore the status quo ante. Chapter “[Managing Environmental Threats: Integrating Nature-Related Risks into Investment Decisions and the Financial System](#)” covers the potential implications of nature-related risks in the financial sector, global economy, and their decision-makers, providing insight into the potential measures that can be adopted to mitigate the risks.

Chapter “[Defense Critical Supply Chain Networks and Risk Management with the Inclusion of Labor: Dynamics and Quantification of Performance and the Ranking of Nodes and Links](#)” focuses on the formulation of a defense supply chain framework using variational inequality theory and the theory of projected dynamical systems that can quantify the resilience of supply chain networks to disruptions in labor. The book continues with chapter “[Facing Shortages: Practical Strategies to Improve Supply Chain Resilience](#)”, which investigates the causes of resource shortages and covers practical strategies to improve supply chain resilience.

Chapter “[Critical Infrastructure Detection During an Evacuation with Alternative Fuel Vehicles](#)” presents an evacuation planning model able to identify critical roads and their fortification using a side-constrained betweenness centrality metric in a heuristic.

Chapter “[Risk Assessment and Identification Methodology for the Defense Industry in Times of Crisis: Decision Making](#)” provides a framework that helps identify and assess risks in times of crisis for corporations that cooperate with the defense industry, while chapter “[Quantum Computers: The Need for a New Cryptographic Strategy](#)” is on the emerging technology of quantum computing and the potential threats that could be exhibited in current cryptography. Chapter “[On the Way to Coastal Community Resilience Under Tsunami Threat](#)” places the focus on potential threats due to tsunami disasters and proposes a toolbox for threat mitigation, and chapter “[Transnational Terrorism as a Threat: Cross Border Threats](#)” covers the topic of transnational terrorism and provides insight into a better understanding of the globalization of terrorist activities.

Chapter “[Resilience Against Hybrid Threats: Empowered by Emerging Technologies: A Study Based on Russian Invasion of Ukraine](#)” provides an overview of the application of artificial intelligence, autonomy, and hypersonics as emerging technologies able to empower hybrid threat activities. In chapter “[Earthquakes: Management of Threats, a Holistic Approach](#)”, a detailed review of the state-of-the-art seismic risk assessment tools is presented. Chapter “[Efficiency Evaluation of Regions’ Firefighting Measures by Data Envelopment Analysis](#)” focuses on the evaluation of disasters due to wildfires based on Data Envelopment Analysis.

Chapter “[Superposition Principle for Tornado Prediction](#)” introduces a model based on the Superposition Principle able to efficiently predict tornados. In chapter “[A Network-Based Risk-Averse Approach to Optimizing the Security of a Nuclear Facility](#)”, the authors present a network-based risk-averse model able to optimize the security of a nuclear facility. Chapter “[Post-disaster Damage Assessment by Using Drones in a Remote Communication Setting](#)” proposes a mixed integer linear programming formulation used to optimize post-disaster damage assessment using drones.

Chapter “[Identifying Critical Nodes in a Network](#)” covers the topic of identifying critical nodes in a network and describes computational methods used in the literature to solve it. Chapter “[Machine Learning-Based Rumor Controlling](#)” provides a detailed review of the efforts to control rumors by using machine learning techniques. The book continues with chapters that include policy issues, such as chapter “[Strategic Communication as a Mean for Countering Hybrid Threats](#)”, which describes Strategic Communication as a tool for countering Hybrid Threats, and chapter “[The Integrated Approach in Countering Contemporary Security and Defence Threats](#)”, which describes the “whole of a government approach,” an integrated methodology to counter security threats, and the approach of citizens’ involvement in national security preparedness for optimal countering of threats.

Chapter “[European Union and NATO Cooperation in Hybrid Threats](#)” includes both NATO’s and EU’s approaches to countering hybrid threats and provides possible ways for closer cooperation for optimal response. Chapter “[Hybrid Threats:](#)

[A European Response](#)” provides a detailed description of the EU’s response to countering hybrid threats using a wide array of tools. Chapter [“Integrated Development Environment Using M&S and AI for Crisis Management E&T”](#) focuses on an AI-based platform developed by CMDR COE that is used for rapid response in a crisis due to disaster. While chapter [“Civil-Military Cooperation for the Countering of Threats: Protection of Civilians During the Development of a Threat”](#) describes a “Total Defense” model that involves citizens in national security preparedness. Finally, chapter [“The Psychological Dynamics of Leadership Amid a Crisis”](#) describes a practical framework able to help leaders make decisions during crises.

The opinions expressed in this book by different authors are not necessarily representative of the opinions of the editors or the publisher. The editors would like to express their gratitude to all invited contributors and their groups who made this work possible. Additionally, we would like to thank the editors of Springer for their efficiency throughout the entire project.

Athens, Greece  
Leuven, Belgium  
Gainesville, FL, USA

Konstantinos Balomenos  
Antonios Fytopoulos  
Panos M. Pardalos

# Contents

<b>Future Threats: Creating a Resilient Society</b> .....	1
Antonios Fytopoulos and Panos M. Pardalos	
<b>Managing Environmental Threats: Integrating Nature-Related Risks into Investment Decisions and the Financial System</b> .....	13
François Gardin and Sven Van Kerckhoven	
<b>Defense-Critical Supply Chain Networks and Risk Management with the Inclusion of Labor: Dynamics and Quantification of Performance and the Ranking of Nodes and Links</b> .....	39
Anna Nagurney	
<b>Facing Shortages: Practical Strategies to Improve Supply Chain Resilience</b> .....	59
Dimitra Kalaitzi and Naoum Tsolakis	
<b>Critical Infrastructure Detection During an Evacuation with Alternative Fuel Vehicles</b> .....	81
Chrysafis Vogiatzis and Eleftheria Kontou	
<b>Risk Assessment and Identification Methodology for the Defense Industry in Times of Crisis: Decision-Making</b> .....	103
Isabella T. Sanders	
<b>Quantum Computers: The Need for a New Cryptographic Strategy</b> .....	125
Britta Hale, Nina Bindel, and Douglas L. Van Bossuyt	
<b>On the Way to Coastal Community Resilience Under Tsunami Threat</b> ...	159
Mark Klyachko, Andrey Zaytsev, Tatiana Talipova, and Efim Pelinovsky	
<b>Transnational Terrorism as a Threat: Cross-Border Threats</b> .....	193
Jake Wright and Silvia D’Amato	
<b>Resilience Against Hybrid Threats: Empowered by Emerging Technologies: A Study Based on Russian Invasion of Ukraine</b> .....	209
Scott Jasper	

**Earthquakes—Management of Threats: A Holistic Approach** ..... 227  
Eva Agapaki

**Efficiency Evaluation of Regions’ Firefighting Measures by Data Envelopment Analysis** ..... 257  
Fuad Aleskerov and Sergey Demin

**Superposition Principle for Tornado Prediction** ..... 267  
Fuad Aleskerov, Sergey Demin, Sergey Shvydun, Theodore Trafalis, Michael Richman, and Vyacheslav Yakuba

**A Network-Based Risk-Averse Approach to Optimizing the Security of a Nuclear Facility** ..... 279  
Eugene Lykhovyd, Sergiy Butenko, Craig Marianno, and Justin Yates

**Post-Disaster Damage Assessment Using Drones in a Remote Communication Setting** ..... 299  
Ecem Yucesoy, Elvin Coban, and Burcu Balcik

**Identifying Critical Nodes in a Network** ..... 325  
Ashwin Arulseivan and Altannar Chinchuluun

**Machine Learning-Based Rumor Controlling** ..... 341  
Ke Su, Priyanshi Garg, Weili Wu, and Ding-Zhu Du

**Strategic Communication as a Mean for Countering Hybrid Threats** ..... 371  
Konstantinos Balomenos

**The Integrated Approach in Countering Contemporary Security and Defence Threats** ..... 391  
Fotini Bellou

**European Union and NATO Cooperation in Hybrid Threats** ..... 405  
Mikhail Kostarakos

**Hybrid Threats: A European Response** ..... 425  
Dimitrios Anagnostakis

**Integrated Development Environment Using M&S and AI for Crisis Management E&T** ..... 443  
Orlin Nikolov and Kostadin Lazarov

**Civil-Military Cooperation for the Countering of Threats: Protection of Civilians During the Development of a Threat** ..... 475  
M. Stette, K. Porath, and S. Muehlich

**The Psychological Dynamics of Leadership amid a Crisis** ..... 521  
Christos Tamouridis, Miguel Moyeno, and William A. Pasmore

# Contributors

**Eva Agapaki** University of Florida, Gainesville, FL, USA

**Fuad Aleskerov** Department of Mathematics, Faculty of Economics, National Research University Higher School of Economics, Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia

Institute of Control Sciences of Russian Academy of Sciences, HSE University, Moscow, Russia

**Dimitrios Anagnostakis** University of Aberdeen, Aberdeen, UK

**Ashwin Arulsevan** Department of Management Science, Strathclyde Business School, Glasgow, Scotland, UK

**Burcu Balciik** Industrial Engineering Department, Ozyegin University, Istanbul, Turkey

**Konstantinos Balomenos** National Defence Policy & International Relations—Hellenic Ministry of National Defence, Peristeri of Athens, Greece

**Fotini Bellou** Department of International and European Studies, University of Macedonia, Thessaloniki, Greece

**Nina Bindel** SandboxAQ, Palo Alto, CA, USA

**Sergiy Butenko** Wm. Michael Barnes '64 Department of Industrial and Systems Engineering, Texas A&M University, College Station, TX, USA

**Altannar Chinchuluun** Department of Finance, Business School, National University of Mongolia, Ulaanbaatar, Mongolia

Institute of Mathematics and Digital Technology, Mongolian Academy of Sciences, Ulaanbaatar, Mongolia

**Elvin Coban** Industrial Engineering Department, Ozyegin University, Istanbul, Turkey



**Silvia D'Amato** Institute of Security and Global Affairs, Leiden University, Leiden, The Netherlands

**Sergey Demin** Department of Mathematics, Faculty of Economics, National Research University Higher School of Economics, Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia

Institute of Control Sciences of Russian Academy of Sciences, HSE University, Moscow, Russia

**Ding-Zhu Du** Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA

**Antonios Fytopoulos** Department of Chemical Engineering, KU Leuven, Leuven, Belgium

School of Chemical Engineering NTUA, Athens, Greece

**François Gardin** Brussels School of Governance, Vrije Universiteit Brussel, Brussels, Belgium

**Priyanshi Garg** Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA

**Britta Hale** Naval Postgraduate School, Monterey, CA, USA

**Scott Jasper** Naval Postgraduate School, National Security Affairs, Carmel, CA, USA

**Dimitra Kalaitzi** Department of Engineering Systems & Supply Chain Management, College of Engineering and Physical Sciences, Aston University, Aston Triangle, Birmingham, UK

**Mark Klyachko** Regional Alliance for Disaster Analysis & Reduction, NPO, Saint Petersburg, Russia

**Eleftheria Kontou** Civil and Environmental Engineering, University of Illinois at Urbana-Champaign, Urbana, IL, USA

**Mikhail Kostarakos** Hellenic National Defence General Staff, Athens, Greece

**Kostadin Lazarov** Crisis Management and Disaster Response Centre of Excellence (CMDR COE), Sofia, Bulgaria

**Eugene Lykhovyd** Wm. Michael Barnes '64 Department of Industrial and Systems Engineering, Texas A&M University, College Station, TX, USA

**Craig Marianno** Department of Nuclear Engineering, Texas A&M University, College Station, TX, USA

**Miguel Moyeno** Teachers College, Columbia University, New York, NY, USA

**S. Muehlich** Concepts, Interoperability, Capabilities, Civil-Military Cooperation Centre of Excellence, Den Haag, The Netherlands

**Anna Nagurney** Department of Operations and Information Management, Isenberg School of Management, University of Massachusetts, Amherst, MA, USA

**Orlin Nikolov** Crisis Management and Disaster Response Centre of Excellence (CMDR COE), Sofia, Bulgaria

**Panos M. Pardalos** Department of Industrial and Systems Engineering, University of Florida, Gainesville, FL, USA

**William A. Pasmore** Teachers College, Columbia University, New York, NY, USA

**Efim Pelinovsky** Institute of Applied Physics, Nizhny Novgorod, Russia

National Research University - Higher School of Economics, Moscow, Russia

V.I. Il'ichev Pacific Oceanological Institute, Vladivostok, Russia

**K. Porath** Concepts, Interoperability, Capabilities, Civil-Military Cooperation Centre of Excellence, Den Haag, The Netherlands

**Michael Richman** University of Oklahoma, Norman, OK, USA

**Isabella T. Sanders** Department of Systems Engineering, United States Military Academy, West Point, NY, USA

**Sergey Shvydun** Institute of Control Sciences of Russian Academy of Sciences, HSE University, Moscow, Russia

**M. Stette** BwConsulting – Inhouse Consulting of the German Armed Forces, Berlin, Germany

**Ke Su** Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA

**Tatiana Talipova** Institute of Applied Physics, Nizhny Novgorod, Russia

V.I. Il'ichev Pacific Oceanological Institute, Vladivostok, Russia

**Christos Tamouridis** Teachers College, Columbia University, New York, NY, USA

**Theodore Trafalis** University of Oklahoma, Norman, OK, USA

**Naoum Tsolakis** Department of Supply Chain Management, School of Economics and Business Administration, International Hellenic University, Thessaloniki, Greece

**Douglas L. Van Bossuyt** Naval Postgraduate School, Monterey, CA, USA

**Sven Van Kerckhoven** Brussels School of Governance, Vrije Universiteit Brussel, Brussels, Belgium

**Chrysafis Vogiatzis** Industrial and Enterprise Systems Engineering, University of Illinois at Urbana-Champaign, Urbana, IL, USA

**Jake Wright** Institute of Security and Global Affairs, Leiden University, Leiden, The Netherlands

**Weili Wu** Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA

**Vyacheslav Yakuba** Institute of Control Sciences of Russian Academy of Sciences, HSE University, Moscow, Russia

**Justin Yates** American Airlines, Fort Worth, TX, USA

**Ecem Yucesoy** Industrial Engineering Department, Ozyegin University, Istanbul, Turkey

**Andrey Zaytsev** Special Research Bureau for Automation of Marine Researches, Far Eastern Branch of Russian Academy of Sciences, Yuzhno-Sakhalinsk, Russia

# Future Threats: Creating a Resilient Society



Antonios Fytopoulos and Panos M. Pardalos 

## 1 Introduction

It is commonly accepted that humanity has had to face some very serious issues in recent years, which are associated, in one way or another, with the pandemic (crisis management, logistics problems [1], work-related issues, healthcare problems for a large proportion of citizens, mass vaccination programs, telecommuting, etc.). As a result, the COVID-19 pandemic has become the cause of a crisis for many people, like none other in recent history. The COVID-19 pandemic was, in other words, a severe crisis that tested to a great extent the capabilities and the fortitude of modern society in a vast range of activities [1]. Certainly, in 2023 when this article is being published, there are still many issues that need to be resolved concerning the pandemic and its impact on the modern world. Huge sums of money have been made available to deal with each crisis, big research programs are ongoing for the treatment of any new mutations of the virus and significant changes have already been made or are about to be made, regarding the operation structure (businesses, government agencies, telecommuting, etc.) [2].

On the other hand, of course, the weaknesses of the systems (administration, logistics, etc.) came to the surface [2], when a crisis occurred that required a wide range of federations, state–private–social–policies, etc., to interact directly as a whole, as if they had been cooperating for years, which had not been required by

---

A. Fytopoulos (✉)

Department of Chemical Engineering, KU Leuven, Leuven, Belgium

School of Chemical Engineering NTUA, Athens, Greece

e-mail: [fytopoulos@chemeng.ntua.gr](mailto:fytopoulos@chemeng.ntua.gr)

P. M. Pardalos

Department of Industrial and Systems Engineering, University of Florida, Gainesville, FL, USA

e-mail: [pardalos@ufl.edu](mailto:pardalos@ufl.edu)

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

K. P. Balomenos et al. (eds.), *Handbook for Management of Threats*, Springer

Optimization and Its Applications 205,

[https://doi.org/10.1007/978-3-031-39542-0\\_1](https://doi.org/10.1007/978-3-031-39542-0_1)

any other kind of crisis in the past to this extent. However, one thing is certain: There is no organization, company, state, or non-state body or individual, who was not directly or indirectly affected by the pandemic and its effects.

Finally, the question that arises after all this is when will we return to normality, a question that afflicts the whole world nowadays. The answer to this question seems to be “not yet,” as humanity will soon have to deal with the indirect, but not insignificant, effects of the pandemic on society and the economy. Ultimately, perhaps the solution is the upgrade of society to a new one – more stable – that will be based on new fundamentals that will be able to respond directly, fast, and effectively in these kinds of crises. In other words, the goal is to create a new, more durable society that is resilient.

The “new normal” seems to be based on the ability of people to “adapt” to new situations. In this context, the exploitation of new technologies to the fullest seems to be a one-way street. Given the adaptation (or else the evolution), humanity is called upon to tread carefully on the new path that history demands for its appointment with the new – fundamentally structured – society, because if this crisis does not become the cause of profound change, it is very likely that at the end of the next crisis there will be only remnants of humanity as we know it today [3]. Therefore, humans may be required to accept a return to normality, but in its new form and not in the old one.

All of the above do not come to creep into a random point of history, but at the point where society seems to be sufficiently “mature” technologically, to have the ability and the tools to face such future dangers that may harm its existence. The rapid development of new technologies in the last 20 years such as Industry 4.0, the Internet of things, 3D printing, advanced-smart materials, biotechnology, machine learning technologies, 5G, artificial intelligence, and robotics provide new “tools,” can and should be used by humans in this direction with the ultimate goal of harmonious cooperation between people and machines in the coming years in light of new upcoming crises and threats.

In this sense, the above developments are not underway due to the pandemic, but are accelerated through it, making it the *catalyst* for the more immediate integration of people into new social-financial demands that will arise. The development and use of emerging technologies will not be maximized because of the pandemic, but the pandemic helps overcome any potential difficulties that might arise and works as a catalyst for the arrival of the new normality. In these complex dynamics, humanity and science are called upon to prepare-open a smooth road, which will lead to the next day safely. In any way though, the threats and dangers lurking are constant and may be identified and dealt with.

In this article, there will not be an attempt to approach the possible new threats from the perspective of the data, but from a more anthropocentric point of view, as our belief is that societies must constantly evolve, using new forms of governance, technology, connectivity, and dealing with threats, but not in a way and to an extent that leads to estrangement and alienation of the human personality. Societies must

protect themselves from the coming threats by constantly evolving and adapting to the new environment, but without being alienated and jeopardized by their own evolution.

## 2 Future Threats

### 2.1 *Challenges in the Use of Artificial Intelligence*

Artificial intelligence can be considered one of the most significant human achievements, although it has yet to be widely integrated into our daily lives – at least in forms that are expected to be used in the coming years. However, it is expected that there will be a huge rise in the AI market in the near future, with China [4] vigorously seeking – if it has not already succeeded – to lead this effort.

As a result, robots are expected to manage a large part of our daily lives in the coming years. Thus, smart systems may constantly provide data, which will have to do with all the devices of our home (IoT), our car, ourselves (IoP), or everything around us (IoE). Similarly, at the working level there will also be a corresponding data flow, which will concern businesses, production–management, logistics, and more. All these data must be collected and analyzed in an effort to make the best possible use of it.

Data have become a new form of “gold” in the modern digital economy, as targeted production can be launched based on them. Ergo, the combination and processing of the data is an essential factor for every business, as they can create new products and services based on the data. In other words, data and their processing provide the information needed to identify possible new needs and create new sources of wealth. The existence of a vast amount of data naturally leads to the immediate need for data scientists who can process and exploit them. Moreover, it raises questions about how and where this information will be stored (e.g., clouds), so that it is easily accessible and avoid the possibility of storing a volume of information that will not be useful.

As every aspect of our daily lives constantly generates data, the solution of creating, a “central system of mass information processing – data” can be a permanent solution. A system that can, through smart algorithms, recognize previously unencountered situations, self-train effectively, and act abstractly within the context of data processing. This allows it to learn from these situations, deconstruct less important aspects, and emphasize essential information.

Artificial intelligence can be, in other words, a great opportunity, but it also can be a great danger, as algorithms may manage everyday situations. In this context, it is worth noting that information systems are defined by their consistency and ability to access information from a large population and therefore may not take into account ethical issues [5]. Policymakers must establish rules governing the creation and development of such algorithms, and humanity can be protected or threatened by [6] these new forms of governance and decision-making.

On the other hand, a significant amount of information and data, which until now had not been taken into account, can now be analyzed to solve complicated problems in various sectors. The use of artificial intelligence algorithms can significantly improve the proper distribution of resources, holistic treatment of climate change, and problems in everyday life, such as our interaction with the health system.

As with anything in life, the use of such methods must be done wisely, as reckless development could lead to the creation of a superintelligent tool that possesses “infallibility” and guides our daily choices based solely on the data, without considering the broader human context –without taking into account that the data concern human lives [6]. Moreover, given the applicability of such technologies in a vast range of work sectors, a large part of professional teams can simply be sidelined by robots leading to jobs being lost on the planet. On the other hand, a greater need for specified working skills will begin to arise, thus reinforcing the successive movements of workers from one sector to another.

The absence of emotions, creativity, compassion, and emotional intelligence on behalf of the machines may easily lead to a state of *robotarianism* (robots + authoritarianism), and if this is not predicted, prevented in time, and taken into account in the initial planning, it may easily lead to isolation and diminished human relationships.

Another significant problem is the algorithm that will be used by the decision-making system, as it will be a black box for the average citizen. There are dangers lurking when humanity depends solely on the decisions of a reliable technological system, but it is not entirely understood how these decisions are made. For example, let us imagine an artificial intelligence system that makes decisions on whether or not to start a war. How confident and how receptive would we be about such an algorithm by allowing it to make such decisions? “Μέτρον ἀριστον” (moderation is the best thing), as the ancient Greeks Cleobulus of Lindos said, meaning we should find the golden mean.

Thus, although decision-making processes can be based on finding the best processes (through well-known optimization algorithms), in some cases it may be preferable not to use these extremums – avoiding extremities and exaggerations. Ultimately, a large part of our daily lives can certainly be “transformed” by the use of artificial intelligence, yet surely people must move forward, but such in a way as to ensure the transparency of the modes of operation, the moral order, the written and unwritten rules of societies and humanity. Since artificial intelligence is here to stay, it is again left up to humans to be able to wisely use this super tool, so as not to create a digital society based only on aggression, competition, and brutality. In other words, the responsibility for using artificial intelligence wisely lies with humans. The failure of an old system can be tolerated by society and can be seen as a good justification for moving to a new status, but the failure of the new one can only lead society to alienation, skepticism, and denial.

## ***2.2 A User-Privileged Society***

The huge development of algorithms that constantly process data has undoubtedly affected people's daily lives. Carefully selected ads based on our preferences are suggested to us daily during the use of our mobile phones. How does the machine perceive what we like and what we do not? Of course through our search history. This means that we consented to the provision of data to the smart algorithms of the Internet (perhaps we should be compensated for this – since we are part of the sales process).

However, there are cases where it is not acceptable to share some of our preferences or choices. The use of personal information from third-party entities or even from the state can lead to threats and societies must establish rules on how far and to what extent it is allowed for the state and private organizations to intrude, learn, process, or share data concerning people and companies beyond the framework of a simple consent on a website.

A modern aspect of such a function that could protect or even become a threat could be the classification of corporations (or even people) based on how trustworthy they are or not and based on social data of personal nature. This way, people can be distributed in different levels of access to social privileges depending on the level of trust of each entity [7]. This has already been implemented in many countries with the establishment of debt control information systems, which define the trust that the financial system can show in individuals or companies based on the management history of their finances and debts.

In a fully digital world, such systems could be extended to other aspects of life, besides financial ones. However, extreme caution is required because we can easily be led to a society of socially privileged entities that will have access to goods and services where others will not. For the proper function of such systems, the fine line that separates “illegal action” from “bad everyday practice” must be made clear from the beginning and the way of possible implementation of such systems for the good of humanity must be examined, in relation to the existence of new cutting-edge technologies (5G, IoP, IoT, biometrics, fingerprint sensors, microchips, facial recognition, etc.) in order to promote and not to pulverize human personality. According to the above, new forms of government could be possible since society will gradually evolve into full digitization. So even at the government level, more technocratic models based on data, rather than ideology, may prevail thanks to their potential for more timely and valid data-based decision-making.

## ***2.3 Pandemics***

We do not need to detail the pandemic as a future threat, as this article is written in the context of COVID-19, whose effects are evident in our daily lives. This is a profound crisis, unlike any faced in recent history. The constant pressure on



healthcare systems and the ongoing lockdowns are driving economies to the brink of collapse. New forms of work, such as telecommuting, have become necessary and the pandemic continues to impact a significant part of our daily lives [8].

This crisis has also taken an unexpected form, namely the issue of trust [9] in scientific data and practices. Some have remained skeptical toward how the pandemic is being handled. The pandemic to date has affected different areas in different ways, both in the private and public sectors. It remains to be seen what other aspects will become visible and what other sectors remain to be affected. For instance, a significant debate is expected to arise later regarding the management of financial issues that have already been maximized, such as debt.

## ***2.4 Climate Change and Major Natural Disasters Due to Extreme Weather***

The modern way of life has led to an ever-increasing demand for energy, resulting in a rise in pollutants and emissions. The more demanding lifestyle and the larger population that tends to live based on the Western model, the rapid development of China, and globalization are intensifying the problem of daily energy waste, leading to energy and climate crises. The climate crisis is one of the most devastating threats to humanity, causing the destruction of biodiversity [9].

On the other hand, the environment provides us with all the resources needed to live, such as water, food, and energy, and ensures their renewal through various necessary processes for humans. Unfortunately, the damage caused to the environment is significant, leading approximately 150 million citizens to change residence due to climate factors, such as global warming by 2050 [10]. The rise in water levels is expected to affect personal property and destroy critical infrastructure of strategic importance in various nations, including roads, railways, ports, the Internet, structures that provide drinking water, tourism, and agricultural cultivation.

Moreover, other natural phenomena directly related to climate change may arise, such as cyclones, droughts, fires, etc. which will become more frequent and intense over time. Of the various future threats, climate change is the one that evolves with long-term effects, which cannot be predicted, and it can affect – like a ticking time bomb – many aspects of human activity. Thus, forms of life can be completely lost from the face of the earth, natural disasters will become more and more severe and frequent, the quantity of available drinking water resources will be significantly affected [11, 12], and rural areas may not be as productive as necessary to meet the growing needs of the population.

These threats are expected to occur initially at a slow pace, but then there is likely to be an exponential rise. This will cause a large part of the population to emigrate, leading to migratory flows [12] due to extreme weather events and rising sea levels, which will also upset the geopolitical relations between states. The next decades are crucial in establishing rules to prevent an environmental disaster,

establish renewable energy sources as the norm, reduce carbon dioxide emissions, and integrate a large part of the population into this way of life.

At the end of the day, humans are both victims and perpetrators of the climate crisis. They must face their own nature and move forward at the pace and tone required by the times. Climate is a powerful arsenal that, if manipulated by “environmental terrorists,” could cause threats humanity has never encountered before.

## ***2.5 The Network of Networks***

As the pace of globalization quickens, more and more networks are developing based on standard communication protocols. This enables people to communicate in different ways with those on the other side of the globe and to send data continuously. At the same time, huge financial, military, and informational systems are based on networks. Through these networks, ever-increasing information flows and millions of new users are inserted and older ones are removed every second. They communicate and make financial trades, leading to the creation of a huge amount of data, which will skyrocket even more with the use of new technologies. This complex system constitutes a patchwork of data concerning businesses, financial institutions, public and private bodies, and ordinary people, which the new society is called upon to manage.

Undoubtedly, a large part of the debate can and must be done around the security of this monstrous complex. In principle, the main nodes that need to be protected [13] must be found to ensure their viability. This huge network interacts with pre-existing and subsequent road, transport, telecommunications, electrical, and other networks. The final result is a vast but magical creation that drives evolution and all other human activities. On the other hand, these same critical nodes of these networks will be targeted by potential malicious actors, seeking maximum damage with the least possible effort. Such cyberattacks can reduce the reliability of the network and make users skeptical about its use.

However, the same question remains: Can and should protection be “imposed” from the outset, given the knowledge of the potential risks, or should we wait for some major negative event that will “necessitate” the introduction of stricter rules for the protection of the network? What would happen if a major cyberattack with devastating consequences on the network (similar to those of COVID-19 in our daily lives) led to the dispute of a major part of the transactions made or the destruction of some cryptocurrencies? It is possible that a large part of humanity that would have been affected would undeniably accept new ways of accessing the Internet, where, for example, multiple confirmations of the physical identity would be required before granting someone access to information on the Internet (e.g., biometrics authentication). In other words, huge threats and crises can lead to enormous “adaptability” and acceptance by users of situations that under normal circumstances might not have accepted. The upsurge in interconnection

automatically leads to the demand for a new society of people, who will interact professionally and personally much more than in the past.

The management of networks is one of the most important areas for human activities in a globalized society. Those who are in complete control of them can intervene in any form of modern activity, disorganizing it and leading it to destruction. This might not be considered as important in some of the individual processes that take place daily, but what if the networks responsible for the operation of financial institutions or the management of nuclear or space stations were compromised? Are humans ready to “sacrifice” less up front on the altar of protection and security to avoid “paying” more in retrospect? Can the use of new methods of biometric surveillance [14] help ensure safer and more controlled access to networks, or will this extend social control to unacceptable levels?

## ***2.6 Control of the Mind: The Next Battlespace***

In recent years, the rapid development of neuroscience, combined with improved imaging techniques of the human mind, has opened new paths in approaching the brain’s functions. Traditionally, the “manipulation” of the human mind was mainly attributed to the media. However, new tools such as neural–interface systems [15] can increase the connectivity of the nervous system with hardware or software, significantly improving a person’s ability to increase their output when interacting with machines.

While such developments can lead to an improvement in the lives of many people with disabilities or increase productivity in industrial processes, they can also be used in immoral ways, such as achieving military objectives. These techniques can be used in military programs to improve and speed up the learning and processing of available data, increase physical endurance and stress resistance, and develop and use prosthetics of upper and lower limbs directly linked to the nervous system. The absence of international laws that clearly define what is legal and what is not, and that outline the limits beyond which such activities cannot be “morally” tolerated, can further enhance the dynamics of these threats. Without proper regulation, these techniques could be used in ways that are harmful to humanity.

## ***2.7 Transnational Organized Crime***

Due to globalization and the continuous increase in networks, the world has been interconnected at a level much higher than ever before. This has created new huge opportunities for profit. However, in parallel with the launch of legal activities, a multitude of illegal activities have also developed. The exploitation of networks

and new opportunities presented in the new era by organized criminal groups has led to maximizing their profits, making this threat extremely serious. International criminal networks exploit supply chains, the Internet, and new technologies for their own benefit, causing problems to the peaceful development of states, threatening the environment, global health, economy, and peace, and ultimately gradually imposing chaos.

Organized crime takes advantage of the Internet's access to data on a daily basis, which can also be used against users themselves. Illegal activities, such as illegal transportation of precious stones, smuggling of oil, weapons, development of drug cartels, poaching, and illegal fishing, are developing exponentially and in parallel with the exponential growth of technology in recent years, as better infrastructure and new technologies can now be used [16]. Of course, in a hyper-connected world, as legitimate businesses are growing and coming together, so does organized crime. It can unite under an international umbrella, further complicating its confrontation.

## ***2.8 A Crisis in Politics: Change in Political Systems***

When everything around us changes, adaptability is essential for stability. One of the main advantages of new technologies is the access of everyone to information and opportunities. Therefore, every day, people originating from different countries, different social groups, or ages now have the same ability to access the whole range of social, professional, and personal activities. Inevitably, given the new possibilities, the interaction of people in new societies is immediate, having much more direct participation in social events, in public affairs, and in decision-making.

Such immediacy has never been so extreme in the past and is likely to lead to a political crisis, with possible changes in political systems. The crisis of today's parliamentary (representative) system may take place soon, leading to more direct forms of democracy, more participatory in decision-making, due to the increased accessibility provided by the new technologies compared to the past, similar to that of ancient Athens.

Inclusiveness is constantly being strengthened, and consequently, more and more of modern society is increasingly interacting in a complex decision-making system. The democratic nature of the Internet is likely to lead to fairer forms of governance, where decisions are made more directly, preventing the predominance of local corrupt elites. In such a crisis, it's possible that politicians themselves may require assistance in finding a solution. This assistance could come in the form of new technological tools that have evolved under the guidance of a technological elite, often referred to as 'elitechs'.

## ***2.9 The Gray Zones Between Truth: Misinformation, Disinformation, and Conspiracy***

Direct access to information also means direct access to its production. Accordingly, people's greater access to the Internet enables them to express themselves more, to influence other people and also to form views and opinions [17]. In this complex patchwork of information, it is normal for facts to mix with opinions, news, and mistaken or forged (accidentally or intentionally) information, often creating confusion.

Hence, the modern human is called upon to develop "senses" that help him distinguish truth from falsehood, news from fake news, and information from misinformation. This means that he needs to distinguish the limits of this gray zone, which can be created naturally or artificially around a piece of information, making the "distinction" of those limits one of the greatest virtues.

As people's dependence on the digital world continues to grow, and for some, their digital lives become 'more important' than their real ones, the significance of distinguishing truth from falsehood becomes increasingly paramount. In this context, modern technologies can potentially help with the development of algorithms based on artificial intelligence or machine learning that will be able to distinguish the real from fake news.

## ***2.10 Space Battles***

Space has always attracted the interest of scientists, leading from time to time to endless "races" for its conquest. However, apart from the well-known thought of the coveted "conquest" of space, we must not forget that a multitude of ever-increasing commercial, military, and government activities use space every day in one way or another, using – among other things – satellites [18] to transmit information.

On the other hand, the development of technology has led to easier access and use of space, thus emerging as a new "field for conflicts" between countries or even between private organizations and this even has led countries to formulate new Departments of Space. Finally, the non-existence of a perfected international space law – accepted by all its users – that will govern and clearly define the rights and obligations of all participants is expected to make the interaction between those involved even more difficult.

## **3 Conclusions**

All in all, taking into account that the new correlations cannot be depicted in their entirety in detail, due to their complexity, the new information age seems to lead

to new challenges for modern people. Threats that until now seemed unlikely or insignificant, in today's interconnected reality can be developed into key threats and dramatically affect the daily lives of people. This was understood with the spread of the COVID-19 pandemic that was a driving force for the evolution of many new forms of work, the operation of institutions and businesses, and the establishment of new problem-solving models.

In this chapter, an attempt was made to briefly describe some of the possible future threats that may affect humankind. Only some of them were described, as the overall list may be inexhaustible. Regardless of whether these threats are related to extreme natural phenomena, pandemics, social upheavals, or relationships between human and machine, what needs to be understood is that significant technological, social, and economic changes in everyday life are imminent, leading to a completely different philosophy of operation. Hence, in the end, modern people will have to "adapt" once again to the new reality, as dealing with all the threats that will arise will make them more resilient to the passing of time.

## References

1. Nagurney, A.: Freight service provision for disaster relief: A competitive network model with computations. In: Kotsireas, I., Nagurney, A., Pardalos, P. (eds.) *Dynamics of Disasters—Key Concepts, Model. Algorithms, Insights*. DOD 2015 2016, vol. 185, pp. 207–229. Springer, Cham (2016)
2. Moosavi, J., Fathollahi-Fard, A.M., Dulebenets, M.A.: Supply chain disruption during the COVID-19 Pandemic: Recognizing potential disruption management strategies. *Int. J. Disaster Risk Reduct.* **75**(February), 102983 (2022)
3. Leach, M., MacGregor, H., Scoones, I., Wilkinson, A.: Post-pandemic transformations: How and why COVID-19 requires us to rethink development. *World Dev.* **138**, 105233 (2021)
4. Lundvall, B.Å., Rikap, C.: China's catching-up in artificial intelligence seen as a co-evolution of corporate and national innovation systems. *Res. Policy.* **51**(1), 104395 (2022)
5. Kazim, E., Koshiyama, A.S.: A high-level overview of AI ethics. *Patterns.* **2**(9), 100314 (2021)
6. Wirtz, B.W., Weyerer, J.C., Kehl, I.: Governance of artificial intelligence: A risk and guideline-based integrative framework. *Gov. Inf. Q.* **2021**, 101685 (2022)
7. Liu, C.: Multiple social credit systems in China. *SSRN Electron. J.* **21**, pp. 22–32 (2019)
8. Nagurney, A.: Perishable food supply chain networks with labor in the Covid-19 pandemic. In: Kotsireas, I.S., Nagurney, A., Pardalos, P.M., Tsokas, A. (eds.) *Dynamics of Disasters. Springer Optimization and its Applications*, vol. 169, pp. 173–193. Springer, Cham (2021). [https://doi.org/10.1007/978-3-030-64973-9\\_11](https://doi.org/10.1007/978-3-030-64973-9_11)
9. Kumar, A., Nagar, S., Anand, S.: *Climate Change and Existential Threats*. Elsevier Inc. (2021)
10. Berchin, I.I., Valduga, I.B., Garcia, J., de Andrade Guerra, J.B.S.O.: Climate change and forced migrations: An effort towards recognizing climate refugees. *Geoforum.* **84**(June), 147–150 (2017)
11. Huang, Z., Yuan, X., Liu, X.: The key drivers for the changes in global water scarcity: Water withdrawal versus water availability. *J. Hydrol.* **601**(January), 126658 (2021)
12. Nagurney, A., Daniele, P., Cappello, G.: Capacitated human migration networks and subsidization. In: Kotsireas, I.S., Nagurney, A., Pardalos, P.M., Tsokas, A. (eds.) *Dynamics of Disasters. Springer Optimization and its Applications*, vol. 169, pp. 195–217. Springer, Cham (2021). [https://doi.org/10.1007/978-3-030-64973-9\\_12](https://doi.org/10.1007/978-3-030-64973-9_12)

13. Arulseivan, A., Commander, C.W., Pardalos, P.M., Shylo, O.: Managing network risk via critical node identification. In: Risk Management in Telecommunication Networks, pp. 1–18. Springer (2007)
14. Babamir, F.S., Kirci, M.: A Multibiometric Cryptosystem for User Authentication in Client-Server Networks. *Comput. Networks*. **181**, 107427 (2020)
15. RoyalSociety: Brain Waves 3: Neuroscience, Conflict and Security. RoyalSociety (2012)
16. Dirks, D., Snyrna, H.F.: Organized crime. In: Encyclopedia of Violence, Peace, and Conflict, pp. 1409–1418. Elsevier, Amsterdam (2008)
17. Aldwairi, M., Alwahedi, A.: Detecting fake news in social media networks. *Procedia Comput. Sci.* **141**, 215–222 (2018)
18. Petroni, G., Bianchi, D.G.: New patterns of space policy in the post-cold war world. *Space Policy*. **37**(April 2015), 12–19 (2016)

# Managing Environmental Threats: Integrating Nature-Related Risks into Investment Decisions and the Financial System



François Gardin and Sven Van Kerckhoven

## 1 Introduction

This book deals extensively with risks and how these can be better managed. One of the great, albeit often overlooked, risks of our current times relate to the environment and its sustainability. This risk plays out in several issue fields, including the financial sector. Calls for greater consideration of environmental sustainability risks to the investment decisions of both the financial sector and separate industries have reached new peaks in the last decade. This follows an increasing awareness of the exposure of investments to a wide set of environmental challenges that impact natural capital assets, natural resources, and the benefits they provide to societies. Addressing these risks requires more than direct policy interventions aimed at reducing public subsidies to activities harmful to the environment. They also require a rethink of capital allocation decisions, with the aim to minimize the adverse impact of private capital flows into activities that are exposed to nature-related risks, while supporting investments for a sustainable environmental transition and adaptation. To that extent, the EU Green Deal and its Sustainable Finance Package explicitly aim at effective capital allocation toward more sustainable activities and meeting the funding gap for financing the transition toward sustainable green activities.<sup>1</sup>

---

<sup>1</sup> The European Commission adopted on April 21, 2021, a package of measures to help improve the flow of monetary resources toward sustainable activities across the European Union [21]. This follows the Action Plan for Financing Sustainable Growth adopted in 2018 [19].

---

F. Gardin · S. Van Kerckhoven (✉)  
Brussels School of Governance, Vrije Universiteit Brussel, Brussels, Belgium  
e-mail: [Francois.Antoine.D.Gardin@vub.be](mailto:Francois.Antoine.D.Gardin@vub.be); [Sven.Van.Kerckhoven@vub.be](mailto:Sven.Van.Kerckhoven@vub.be)



In the annual global risk survey conducted by the World Economic Forum [62],<sup>2</sup> environmental risks such as climate change and biodiversity losses are now ranked among the top risks by economic and financial decision-makers. This echoes the fact that many of the environmental threats that trigger the risks financial institutions face in the twenty-first century tend to exhibit new characteristics, such as larger scale, increased likelihood, and deeper interconnectedness [7].

In this context, financial authorities and market participants have started to review their exposure to a wide set of environmental risks, looking in particular at policies providing for the enhancement of risk assessments and their disclosure to the public and authorities. For example, financial institutions must increasingly integrate new regulations aiming at greater disclosure and integration of nature-related risks, such as the Sustainable Finance Disclosure Regulation (SFDR) introduced in the EU in 2019 [20]. Complimentarily, some market-led initiatives have emerged, such as the special Taskforce on Nature-Related Financial Disclosures (TNFD),<sup>3</sup> which aims to develop a risk management and disclosure framework for organizations to report and act upon evolving nature-related risks.

These initiatives bring to the front the following questions: How can nature-related risks be assessed more coherently and consistently, and how can they be integrated by financial institutions in their investment and lending decisions, capital allocation decisions, and their advisory to, and engagement with, the companies they finance? Is the nature of these risks sufficiently understood by financial institutions and are the formulated responses adequate?

In this chapter, we first take stock of the current state of the literature. We look at the definitions and key characteristics of nature-related risks. We also consider the systemic nature of nature-related risks due to their interdependencies, and how this complexity can lead to more systemic risks, either exogenous or endogenous to the financial system.

This chapter then looks at the current practices of financial institutions and in particular their limits in enabling a solid consideration of nature-related risks for their investment decisions. We look at what measures are being promoted to address nature-related risks and to what extent these risks call for specific responses in terms of threat management. In doing so, the chapter takes stock of the developing practices and recent studies to better identify, assess, and integrate nature-related risks and the potential ways forward. Finally, this chapter also looks

---

<sup>2</sup> Published on a yearly basis by the World Economic Forum, the Global Risks Report series tracks global risks perceptions among risk experts and world leaders in business, government, and civil society. It examines risks across five categories: economic, environmental, geopolitical, societal, and technological. In 2022, the top three risks are all nature-focused (climate change, extreme weather, and biodiversity loss) and five of the top 10 risks relate to environmental challenges (including human environmental damage and natural resource crisis).

<sup>3</sup> The TNFD is a global, market-led initiative with the mission to develop and deliver a risk management and disclosure framework for organizations to report and act on evolving nature-related risks, with the ultimate aim to support a shift in global financial flows away from nature-negative outcomes and towards nature-positive outcomes [59].

at the opportunity of using precautionary approaches to deal with the uncertainties of nature-related risks.

## 2 Literature Review

This literature review provides a review of both academic papers and policy-oriented research by public authorities and by financial market participants. There is an expanding set of studies aiming to build awareness of the magnitude of nature-related risks for the financial sector and the economy. These studies go beyond analyzing the impact of climate-related risks by looking at a wider set of environmental risks and the systemic nature of these risks. To that extent, recent studies have been carried out on the economic and financial impact of environmental changes [12, 44]. Complimentarily, the risks environmental events can generate for financial stability have slowly attracted some [5]. Increasingly, greater recognition is also given by central banks and regulators to the risks these pose to the financial system [29]. For instance, there were comprehensive studies carried out by the Dutch central bank [59] and the French central bank [55] on the exposure of their financial system to nature-related risks, focusing on biodiversity. These studies overall call for greater consideration in managing these risks.

There are several studies that provide a wide variety of concepts that are instrumental to analyze nature-related risks and their characteristics. The clarification of this set of evolving concepts used to analyze the relationship between nature, investments, and the economy is necessary and will become substantially more important as a diversified group of stakeholders starts to apply these concepts on a more systematic basis. This includes for instance clarifying the concept of natural capital or the notion of ecosystem services [2, 6, 10, 39], which will be explored later in this chapter. There are also studies that review the evolving concepts used to identify the types of risks involved and their link to financial practices [9]. When it comes to the characteristics of these risks, several studies point to their unique characteristics and the importance of their inclusion into the risk management practices of the financial sector [31, 61].

Other than studies demonstrating the importance of the inclusion of nature-related risks, several studies have also studied the current financial practice to assess and address the latter [17, 42, 43]. A relatively large number of studies look at current Environment, Sustainability and Governance (ESG) and Corporate Social Responsibility (CSR) frameworks and investigate how these are implemented by the financial industry ([36, 45, 49, 51]. In particular, some studies look into the current limits faced by institutional investors in integrating environmental sustainability in the long term [53]. Moreover, financial regulators have conducted specific reviews of the practices in terms of addressing environmental risks. For instance, the European Central Bank has published guidance in relation to the supervisory expectation for banks to better manage these risks [16].

However, several questions remain unanswered at large. First, it appears that the actual “transmission” mechanisms between environmental risks and the economic and financial system could be the subject of further empirical research. Only limited research has been carried out to establish and conceptualize the linkages between the economic (human) activities and the related environmental pressures, and the interdependency between both. More attention still needs to be devoted to analyze the exposure of economic agents to, for example, ecosystem services [11]. In particular, biodiversity loss has so far not been subject to in-depth research from the financial risk angle [3]. Systemic risks also need further investigation when it comes to areas such as contagion between the financial system, the real economy, and their potential consequences on the environment. The importance of systemic supply chain risks has been highlighted [50], but further research is needed to understand the potential ripple effects of nature-related dependencies and impacts.

Several studies highlight the necessity for the financial sector to increase its capabilities in identifying, measuring, assessing, and mitigating nature-related risks (such as [8, 41, 43]), as well as the potential to integrate natural and environmental factors into their investment strategies [52]. Financial theory has already looked into the limits of current standard risk management practices and the opportunity to incorporate new paradigms to address “wild” risks, which are disruptive and scalable [37]. These aspects should be further investigated through applied research, in order to better understand the potential way forward to better integrate nature-related risks and opportunities in financial decisions.

Finally, it seems that the current decision-making mechanisms and governance pitfalls that may account for market failures are still to be further investigated. New aspects pertaining to nature-related risks could be further researched such as what currently drives decisions made by investors considering these risks? How are the nature-related risks processed and internalized by the financial markets and investors? Which areas could be improved?

### **3 The Evolution of the Concepts Defining Nature-Related Risks**

To be able to manage any risk, and nature-related risks in particular, clarity is first needed with regard to what exactly the different concepts mean. Indeed, several concepts have been developed to characterize the risks related to the natural environment, but it appears that these concepts and their link to financial decision-making still need to be further clarified and investigated empirically.

First, it is important to define the notions and limits of the concept of nature-related financial risks. This terminology is increasingly used in the context of sustainable finance and increasingly so as a substitute for environmental risks. The concept is primarily related to the risks caused by nature loss and environmental

degradation. This implies a necessity to be able to measure the losses that relate to changes in the state of nature. To that extent, nature may be envisioned as a form of capital, along with financial, social, and cultural capital. The Natural Capital Coalition [40]<sup>4</sup> defines natural capital as the “stock of natural ecosystems on earth including air, land, soil, biodiversity and geological resources which underpins our society by providing value for people both directly and indirectly.” Using this approach, nature-related financial risks can be defined as risks that arise from changes in the condition of natural capital and the benefits these assets provide, as well as societal responses to these changes.

However, this highlights the need for a robust definition of natural capital and what it entails. The notion of natural capital itself has been an evolving concept over time [39]. The concept was first developed to incorporate natural constraints into the economic lexicon, allowing economists to take into account finite and renewable natural resources, and their contribution to economic activities. A concept intrinsically related to natural capital is the notion of ecosystem services. Ecosystem services are the ecological characteristics, functions, or processes that directly or indirectly contribute to human well-being: that is, the benefits that people derive from functioning ecosystems [10]. This includes services such as food provision, natural water treatment, pollination of crops, or fertile soil which are vital for agricultural and industrial business processes. A Common International Classification of Ecosystem Services (CICES) was developed from the work on environmental accounting undertaken by the European Environment Agency (EEA).<sup>5</sup> According to this classification, ecosystem services can be categorized as provisioning services (such as the biomass for nutrition, materials and energy, or water), regulating services (such as flood control, storm protection, water purification, and climate control), and cultural services (such as physical and experiential interactions with the natural environment).

The concept of natural capital is already used sporadically and narrowly to include the environment as part of economic valuation. However, it can also be argued that natural capital and its benefits encompass a set of immutable natural items satisfying basic needs, which are critical and non-substitutable, and as such cannot be valued in a limited way [39]. This has been the view of ecological economists arguing for a strong sustainability view of natural capital, whereby losses cannot be quantified in simple monetary terms. Furthermore, natural assets cannot be fully assessed in a direct and static way given their evolutionary dynamics and their complexity. Following that approach, the notion of nature-related risks should be extended beyond utilitarian models to include impacts, which are uncertain and long-lasting.

---

<sup>4</sup> The Natural Capital Coalition is collaboration between leading organizations in research, science, academia, business, advisory, membership, accountancy, reporting, standard setting, finance, investment, policy, government, conservation, and civil society. It established a protocol in 2016, which is a standardized framework for businesses to identify, measure, and value their direct and indirect impacts and dependencies on natural capital.

<sup>5</sup> For further information, see the structure of CICES at <https://cices.eu/cices-structure>

Once they have been related to the evolving state of nature, the definition of nature-related financial risks also requires a clarification of what types of risks fall under its scope. For instance, the Taskforce for Nature-Related Financial Disclosures ([56], p. 34) defines nature-related risks as “the potential threats posed to an organisation linked to its, and other organisations’, dependencies on nature and nature impacts. These can derive from physical, transition and systemic risks.” Physical risks are related to the dependence of economic activities on the condition of nature and ecosystem services, whereby a declining state of nature leads to negative impacts on these economic activities. The physical risk of loss of ecosystem services can indeed threaten companies and production processes dependent on them, create supply (and demand) shocks, and ultimately translate into a deterioration in their financial position. To that extent, the agricultural and forestry products’ sector appears most directly dependent on nature [58], with a very high dependency on three types of ecosystem services: direct physical inputs such as water for crop irrigation or livestock, or fibers like wood for timber; services that enable production such as pollination for agricultural products, nursery habitats for aquaculture and fishing; and services that provide protection from natural hazards such as floods (e.g., from mangroves for aquaculture). Another highly dependent sector is the energy and utilities’ sector that are contingent on water flow maintenance and natural protection from disruption.

In addition, a definition of nature-related financial risks based on natural capital should clarify how the physical impacts of natural risks or hazards are included in the physical risk assessment, beyond the risk of deterioration and losses of ecosystem functions and benefits provided by natural capital. Independently on how human activities may value and protect natural capital assets, natural hazards (such as earthquakes, floods, fire, storms, and diseases) will occur, leading to material financial risks and losses for economic activities. It is important to link these to the state of natural capital, since anthropogenic processes and activities contributing to environmental degradation can lead to increasing likelihood and impact of natural disasters. For example, deforestation and further deterioration of ecosystems that contribute to massive carbon storage may eventually contribute to increased climate risks. Beyond providing climate regulation benefits, the ecosystem functionalities can also play a major role in mitigating the impact of natural risks by lowering vulnerability, such as by providing natural protection against floods or storms. Sectors with physical assets that are exposed to natural hazards (such as the real estate and infrastructure sector) can be highly vulnerable to these risks.

On the other hand, the negative impacts on the nature of activities and companies may lead to transition risks, as a result of potential shifts toward more sustainable models in policy, technology, and changing consumer and investor preferences. Companies may face reputational risks when they are perceived as contributing to environmental degradation or when they lag in terms of transition. Tighter environmental regulatory standards may also lead to increasing liability and litigation risks for companies whose activities have a negative impact on the environment. In its

review, the Dutch Central Bank points to the Dutch nitrogen crisis as a case study of nature-related transition risk, whereby regulation has been introduced in 2020, which will bring about a reduction in nitrogen emissions and where measures show that nitrogen-emitting sectors will have to help achieve the reduction. These sectors account for around 39% of total lending in the Netherlands [59].

In terms of impacts, some argue that the risks should not be limited to their financial impact, but also to the wider sustainability impact and risk they may cause for society, regardless of whether these externalities result in a financial risk for the investments. This approach is coherent with the concept of “double materiality” introduced in the Non-Financial Reporting Directive (NFRD) of the EU,<sup>6</sup> where companies not only need to report on environmental risks, which are financially material, but also on risks, which have external impacts on the sustainability of the environment, which may eventually lead to additional physical or transition risks for society.

Ultimately, nature-related risks may trigger systemic risks for the stability of the economic and financial systems. Systemic risk in this case can be defined as the risk of collapse of an entire financial or economic system, as opposed to risk associated with any one individual entity, group, or component of a system, which can be contained therein without harming the entire system. Systemic risks are also relevant for environmental risks per se, given the interlinkages between ecosystems and the complexity of nature systems. These risks relate in particular to the systemic impacts of the loss of ecosystem functions and biodiversity [64] (Tables 1 and 2).

Considering these various components (summarized in Table 1), one may define the total nature-related financial risk of an economic activity as the sum of the physical risks and transition risks pertaining to the activity, as well as the systemic risks and external nature-related impact risks the activity may trigger for society at large. For a specific company, its nature-related sustainability risks may not necessarily translate into financial risks as potential costs may not be internalized. However, they trigger costs for other agents and society overall. The level of systemic risks for the company will depend on its exposure to systemic risks, which affect the entire financial and economic system. When these costs are summed up at the level of society, the total costs will include all physical costs (both related to loss of ecosystem functions and incremental costs of natural disasters), transition costs, and systemic costs.

---

<sup>6</sup> Directive 2014/95/EU on the disclosure of nonfinancial and diversity information (referred to as the “Non-financial Reporting Directive” – NFRD). On April 21, 2021, the Commission adopted a proposal for a Corporate Sustainability Reporting Directive (CSRD), which would amend the existing reporting requirements of the NFRD.

**Table 1** Components of nature-related financial risks

Risk type	Definition	Examples
Physical risk linked to natural ecosystem service loss and aggravated risk of natural hazards	Physical risks that arise from the loss of ecosystem services, such as provisioning services, regulation, and maintenance services, on which the activities may depend to function Deterioration of nature may also lead to incremental physical risks that arise from extreme events such as geophysical hazard (weather) or biological (disease) – and disruption of longer-term conditions	Depletion of wild fish stocks, soil degradation, loss of natural coastal protection (such as mangroves), <i>deforestation</i> Impacts of floods, storms, heat waves, droughts, wildfires, diseases, rising sea levels (longer term)
Transition risk (internalized)	Risks that arise from societal efforts to address nature-related impacts and externalities, mainly through changes in public policies, changes in consumer and investor preferences, technology, and innovation shifts	Environmental restrictions, pollution control regulation, environmental taxation, changing consumer demand, shift to clean energy, and transportation technologies
Environmental sustainability risk external to the company	The sustainability risks are the potential impacts and externalities of organizations on natural capital over the long run and costs for society overall, which may not be internalized and fully translate into financial impacts for the organization via internal physical or transition risks (consistent with the principle of double materiality)	Activity pressures such as GHG emissions, land use, pollution, marine ecosystem use, and disturbances, can lead to long-lasting impacts on the environment and causes deterioration of natural capital
Systemic risk	Explored later in the chapter, systemic risks in financial terms can be defined as the risk of collapse of an entire financial or economic system or entire market, as opposed to the risk associated with any one individual entity, group, or component of a system. Systemic risks are also relevant for environmental risks per se, with complex interactions, potential domino effect, and contagion between ecosystems	Impacts on the real economy leading to financial risk with contagion within the financial system, potentially impacting in turn the economy Transmission of risks via supply chains: nature-related impacts on agriculture transmitted to food processing and distribution, apparel, leading to potential disruptions and cost pressures Interdependency between climate risks and biodiversity risks

**Table 2** Underlying notions

Function type	Definition	Example
Natural capital	Stock of renewable and non-renewable resources that combine to yield a flow of benefits to people, referred to as ecosystem services (NCC definition)	Biological, mineral, and physical resources: plants, animals, soils, minerals, land, freshwater and marine ecosystems, atmosphere
Natural hazard	Natural phenomenon that can have a negative effect on humans and other animals, or the environment. Natural hazard events can be classified into geophysical and biological. Natural hazards can be provoked or affected by anthropogenic processes	Floods, storms, heat waves, droughts, wildfires, diseases, rising sea levels (longer term)
Ecosystem service	Benefits that people obtain from natural capital, from provisioning to maintenance and regulation services, or cultural services	Air and water purification services, crop pollination, and the breaking down of waste
Nature-related impacts	Impacts relate to how economic activities may affect natural capital and ecosystem services, by contributing to certain environmental pressures	Contribution to pressures such as climate change, ecosystem use, resource over-exploitation, pollution, or invasive species
Nature-related dependencies	Dependencies relate to how economic activities and business processes may rely on ecosystem services and natural capital	Dependencies of business processes on ecosystem services such as natural resource provision (e.g., fishing), natural protection (e.g., coastal infrastructure), or cultural services (e.g., tourism)

## 4 Tackling the Specificities of Nature-Related Risks

Beyond the current conceptual confusion, it is important to look at the characteristics that underlie these risks and what their implications are for the economic and financial sectors. Those financial implications are still to be investigated empirically [3].

An important characteristic of nature-related risks is the two-way relationship. On the one hand, economic activities are dependent on the services the environment provides them, leading to physical risks in case of ecosystem deterioration. On the other hand, economic activities are also impacting environmental degradation leading to increased risks for exposed companies. If companies transition to more sustainable models, some of the physical risks should be offset. For instance, by



reducing their emissions of water pollutants, water-dependent industries may also ensure the future availability of clean water resources for their own use, but this all depends on the timeframe and characteristics of the transition itself, as delays in the transition may well generate physical risks before potentially higher transition risks are to be incurred. The latter may be due to the need for corrective and disorderly actions at higher costs, following a similar pattern to the “too little too late” scenario outlined for climate risks [42, 43]. Moreover, at the level of a specific economic activity, the dependency risks linked to specific ecosystem functions may not be related to the impact it has on ecosystems’ functions, making these risks asymmetric. For instance, the plastic-producing industry has a major downstream impact on marine ecosystems but is only marginally dependent on marine living resources and impacted ecosystem services. The ENCORE<sup>7</sup> database provides an extensive mapping of sub-industries and business processes according to their respective direct ecosystem dependencies and nature-related impacts, which shows the complexity and potential asymmetries of these relationships.

Nature-related risks, either physical or transition risks, can prove to be challenging to anticipate and assess in terms of likelihood and impact. First, there is a lack of extensive historical data that can be applied to risks that are dynamic, driven by evolving dynamics of environmental degradation and the corresponding societal responses. Like climate challenge, it is challenging to build models without historical data to extrapolate and be able to rely on robust models to develop a forward-looking view. In that respect, the Bank for International Settlements [26] highlights in a recent study some key challenges for conducting stress tests on climate risks, which include data availability and reliability, the adoption of very long-term horizons, the uncertainty around future pathways of key reference variables covering physical risks, and the uncertainty related to transition risks and challenges in modeling approaches.

Nature-related risks in particular are highly complex due to the multiple pressures and threats at play, leading to dynamic interactions. Compared to climate risks, multiple metrics are required to track multiple problems, over different time and spatial scales, and types of environments [31]. In particular, these risks are characterized by complex spatial distributions of impact. Indeed, the activity causing an environmental degradation impact may be located in a different place than where the impacted activities or assets are, and the overall spatial impact can be difficult to measure. An illustration of this challenge of measuring spatial impact is the conundrum of what happens to plastic waste when it enters the ocean. A comprehensive study shows the major gaps in being able to measure and locate the amount of plastic emitted to the environment at an aggregated level, based on a global model of ocean plastics from 1950 to 2015 [35]. When it comes to a specific

---

<sup>7</sup> ENCORE (Exploring Natural Capital Opportunities, Risks and Exposure) is a tool to help users better understand and visualize the impact of environmental change on the economy [25]. It was developed by the Natural Capital Finance Alliance in partnership with UNEP-WCMC.

project or activity, locating the impact of waterborne or airborne pollution pressures may prove extremely challenging.

Furthermore, an important dimension to consider for risk managers and policy-makers is the long-term potential of nature-related risks and how these risks may develop over time. Certain risks may be insignificant when measured over a short-term horizon but build up incrementally over longer cycles, such as the changes in the climate regulation function of nature (sequestration of greenhouse gases) or the mass stabilization and erosion control functions of ecosystems, which does not preclude that some physical or transition risks have already been materializing. For instance, invasive species have already been responsible for substantial biodiversity decline and high economic losses and costs to society. The total reported cost of these has reached a minimum of US\$1.3 trillion over the past few decades (1970–2017), with an annual mean cost of US\$26.8 billion, which includes the costs to manage and adapt to these threats [13].

Future pathways have to be understood, which is particularly challenging for nature-related risks due to their nonlinear form. This is notably a consequence of the complex interactions at play, where compounding effects or sudden accelerations can take place. Slow-building trends or events, such as the deterioration of a specific ecosystem, can increase slowly but gain momentum over time in a nonlinear fashion. At the global level, the notion of “tipping points” or planetary boundaries has been developed, where crossing these boundaries increases the risk of generating large-scale abrupt or irreversible environmental change [48].

By their disruptive nature, which may for instance be caused by sudden losses of ecosystem services, emerging societal or technological responses, or the unexpected developments of major and persistent environmental pressures and societal responses over the long run, nature-related risks may be unfit for standard risk measurement approaches. Financial and economic literature has already demonstrated the limits of Brownian models and standard “random walk” approaches to account for financial risks [37], due to exceptional events or the lack of continuity and linearity over time. Some authors argue for these types of nonstandard risks can have disproportionate impact to be much better integrated by financial market participants [38]. To that extent, “power-law” distributions may be more fit than normal and Poisson distributions and averages, to capture the potential “fat tails” of nature-related risks and integrate disproportionate events that can impact certain businesses or locations. Some authors [60] argue for sustainable financial risk models that are more suited for the nature of risk profiles and their “fractal” nature.

Overall, it appears that nature-related risks may be hard to predict and disruptive. Accepting the statistical distribution and unique characteristics of these risks has major implications in terms of methods to be developed by the financial sector, above and beyond standard risk management approaches. To that extent, the concept of the “Green Swan” has been introduced for environmental risks and specifically climate-related risks by the Bank for International Settlements [5] whereby potentially extremely financially disruptive environmental events could be behind the next systemic financial crisis.

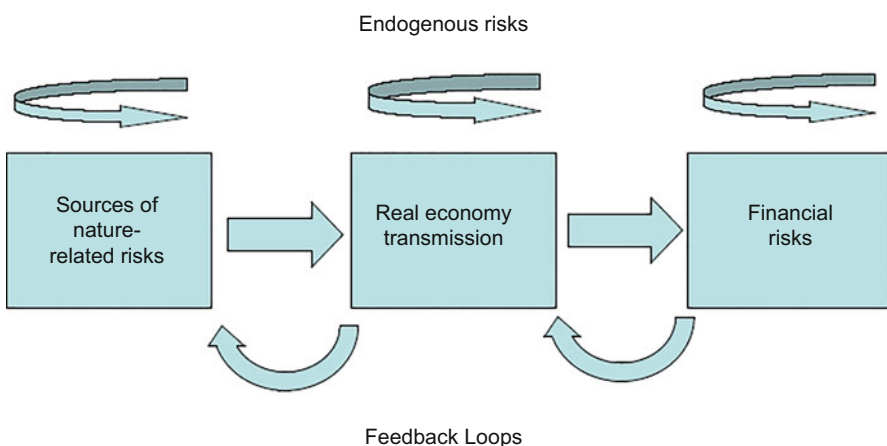
## 5 Transmission Channels and Potential Systemic Risks for the Stability of the Economic and Financial Systems

Nature-related systemic risk includes the exogenous nature risk to the smooth functioning of the economic and financial system and the risk created endogenously by the financial and economic systems, respectively (as illustrated in Graph 1). In addition, as mentioned earlier in the chapter, endogenous systemic risk is also part of the environmental sources of risk.

Key transmission channels for nature-related risks into the real economy include the impairment of assets and collateral, as well as lower corporate profitability due to lower revenues, higher costs, and potential liability risks. Households may also be impacted given the potential loss of income from weather and climate changes and the impact on health, labor market frictions, and property damage. Above and beyond the microeconomic impacts on businesses and households, natural risks may also have a macroeconomic impact in terms of inflation, investment flows, and productivity [42, 43, 55].

As stated before, systemic risks also develop within the real economy, given the interdependencies of value chains, and the indirect exposure of economic activities to each other when facing multiple nature-related risks. The systemic nature of supply chain risks [50] may lead to ripple effects. This means several “feedback loops” are to be considered within the real economy.

For instance, the dependency risk faced by the agricultural sector can have repercussions across multiple industries processing agricultural commodities, which then supply other industries. Multi-regional input–output tables may thus be used to model these supply chain exposures. Considering the direct dependencies, a recent study from the French central bank [55] finds that 42% of the market value of securities held by French financial institutions comes from issuers (nonfinancial



**Graph 1** Systemic risks spanning from environmental sources of risks to the real economy and the financial system

corporations) that are highly or very highly dependent on at least one ecosystem service and that considering the upstream (or indirect) dependencies to ecosystem services, all security issuers in the banks' portfolio are at least slightly dependent to ecosystem services through their value chains. The study finds that the banks' portfolio mainly depends on ecosystem services related to the provision of water (surface water, groundwater) and on the "maintenance and regulation" type of ecosystem services such as mass stabilization and erosion control, flood, and storm protection, and climate regulation. This is also consistent with the findings of the Dutch Central Bank review, which highlights that 36% of the portfolio of Dutch financial institutions appears to be highly or very highly dependent on one or more ecosystem services, with the highest dependence on services that provide ground and surface water [59].

These impacts on the real economy may eventually lead to market, liquidity, credit, underwriting, and operational risks within the financial system [42, 43]. As nature-related risks impact business assets and operational margins, this may limit their ability to generate profits and cash flows and raise capital and repay debts, which will eventually lead to market, liquidity, and credit risks for financial institutions. In addition, for insurers increasing insurance losses and gaps may lead to underwriting risks. Finally, financial institutions may face increasing operational risks in terms of compliance, litigation, and reputational risks. These financial risks may subsequently lead to systemic risks within the financial system, as the financial difficulties of some financial institutions may see a contagion effect on the financial system as a whole in ways similar to the 2008 financial crisis [63].

Beyond the endogenous systemic risks at the level of each system (environmental, economic, and financial) and existing transmission channels from nature to the real economy and the environment, feedback effects are also to be considered. For instance, if the credit rating of a sector exposed to nature-related risk is lowered, behavior in the real economy that further damages nature could end up being promoted [7]. In the case of the agricultural industry, a lower rating and higher interest rates could deter investment in equipment that improves the productivity of degraded land, in turn increasing the likelihood that more land is deforested to meet food demand.

Finally, systemic risk also leads to a financial risk that cannot be diversified. From a portfolio management perspective, this will imply more systematic risk (beta), which cannot be efficiently diversified across the assets in the portfolio and need to be factored in the capital asset pricing model. How such a risk premium is integrated in the valuation of the assets, and to what extent it may vary across sectors and geographies still has to be empirically evaluated.

## 6 Current Practices and Their Limits

Financial institutions have been mainly integrating environmental risks into investment decisions under the umbrella of the Environmental Social and Governance (ESG) framework. By applying this approach, financial institutions seek to evaluate

the environmental, social, and governance characteristics of the companies and projects they invest in (or lend to). To do so, they analyze a wide set of sustainability factors, including the environmental risks pertaining to sectors of the economy. To implement this type of approach, they currently mainly rely on corporate social responsibility (CSR) frameworks, the actual reporting from the investee companies, and their adherence to specific industry and sustainability standards. Within the types of environmental risks that are considered, climate risks and exposures to carbon emission pressures have been given specific and growing attention [42].

However, in its “Overview of environmental risk analysis by financial institutions,” the Network for Greening the Financial System [43]<sup>8</sup> reported that only a fraction of large financial institutions in OECD countries and China have begun to implement some Environmental Risk Assessment (ERA) methods for assessing environmental risks and that many of their applications have remained at the experimental stage. Among the reasons given for the lack of effective environmental risk assessment practices by these financial institutions, there is their limited understanding of processes by which environmental risks can ultimately translate into internal financial risks, and how to quantify such risks. One example of a positive development in that direction is the assessment tools provided along the Natural Capital Coalition Protocol [40, 41] to help businesses to measure and value the environmental services that they rely on and their natural capital liabilities, which include the environmental damage that may result from their operations.

One of the key barriers for financial institutions and investors is the gap in terms of data availability and quality. When it comes to better accounting for nature-related risks, access to sufficient and actionable data has been identified as a critical limitation for financial market participants [47].<sup>9</sup> As a result, traditional risk management techniques relying on the extrapolation of data cannot be applied properly. Currently, many nature-related risks do not fall under the reporting obligations of companies. Most disclosures are voluntary and have been encouraged by frameworks such as the Sustainability Accounting Standards Board (SASB). In the future, it is envisaged that additional metrics will be included under new regulations such as the proposed Corporate Social Responsibility Directive (CSRD) in the EU.<sup>10</sup> Parallel to corporate disclosures, primary data on the environmental

---

<sup>8</sup> The Network is a grouping of Central Banks and Supervisors on a voluntary basis, whose purpose is to help strengthening the global response required to meet the goals of the Paris Agreement and to enhance the role of the financial system to manage risks and to mobilize capital for green and low-carbon investments in the broader context of environmentally sustainable development. To this end, the network defines and promotes best practices to be implemented within and outside of the membership of the NGFS and conducts or commissions analytical work on green finance.

<sup>9</sup> According to a survey conducted by Responsible Investor and Credit Suisse, data are the biggest barrier to making investments that support biodiversity, with 77% of 222 investors putting it above being unable to value natural capital and lacking internal expertise (Unearthing Investor Action on Biodiversity, conducted in collaboration with The Nature Conservancy, the Zoological Society of London and the International Union for the Conservation of Nature, January 2021) [47].

<sup>10</sup> On April 21, 2021, the Commission adopted a proposal for a Corporate Sustainability Reporting Directive (CSRD), which would amend the existing reporting requirements of the Non-Financial

impact, and an estimation of the contribution of the business processes employed and activities, and the geolocation of these activities should be used. To that extent, new techniques in the field of satellite imagery and remote sensing are being developed to track more systematically the nature-related impacts of industrial activities. Extensive methodologies have been developed for estimates of carbon emissions, and new methodologies have also been developed to be able to better quantify the economic activities' impacts on natural capital and biodiversity [34].

Moreover, in terms of data, financial institutions rely to a large extent on the "curated" data provided by external ESG rating agencies, as opposed to dealing with primary environmental data. In terms of data, many ESG data vendors rely heavily on counterparties' self-reported information, which may not be sufficiently reliable. Moreover, there is a challenge in terms of the objectivity of the data, as shown by the lack of correlation in scores between rating agencies [4]. For instance, across six large rating agencies,<sup>11</sup> there is only a correlation of 0,53 (Pearson) between the ratings on the environmental dimension. One major issue for ESG ratings is the inconsistency in data definitions and methodologies between different data vendors [42, 43]. Berg et al. [4] found that the different ways ESG criteria are measured explain more than 50 percent of the variations across ESG ratings.

Another limitation for financial institutions is the integration of these risks in their actual decision-making processes. First, it is unclear how these risks can lead to actual changes in the valuation of financial assets and decisions and to what extent these risks can be priced in, and internalized, given their complexity. Traditional investment approaches are essentially geared for capturing financial value in terms of financial risk and return, with a focus on short-term returns. In that approach, the measure of financial risk is rather narrow [52, 53]. Many investors still consider ESG as an add-on to financials and business models, instead of it being a driver. The long-term horizons of these risks are also an issue, given the relatively short average time horizons of investment strategies and loan books. Furthermore, when applying discounting factors over long-term horizons, their financial materiality may be significantly reduced.

Current practices to integrate nature-related risks also include capital allocation decisions. Certain nature-related risks may already be included in the screening criteria in place for investments or loan applications. To that extent, a number of financial institutions in the EU have started to exclude the financing of fossil fuel-related activities. For instance, 129 of the 1000 largest European pension funds have issued a divestment statement of fossil fuels (13%), accounting for approximately 33% of all pension assets [14]. Another example is the European Investment Bank (EIB) 2019s decision to end its financing of oil, gas, and coal projects after 2021,

---

Reporting Directive (NFRD). In particular, it introduces more detailed reporting requirements and a requirement to report according to mandatory EU sustainability reporting standards.

<sup>11</sup> KLD, Sustainalytics, Moody's ESG (previously Vigeo-Eiris), S&P Global (previously RobecoSAM), Refinitiv (previously Asset4), and MSCI.

a policy that will make the EU's lending arm the first multilateral lender to rule out such investments. Moreover, a higher proportion of investment flows are into investment strategies that embed environmental criteria in their objectives. For instance, in 2020, the majority of net investment fund flows in Europe went into funds that have sustainability characteristics.<sup>12</sup> However, objective criteria still have to be defined when it comes to considering the nature-related risks in the screening of investments. To that extent the EU Taxonomy<sup>13</sup> creates a framework for a criteria-based approach to defining "sustainable" environmental investments considering six environmental objectives. They range from climate change mitigation, climate change adaptation, the sustainable use and protection of water and marine resources, the transition to a circular economy, pollution prevention, and control, to the protection and restoration of biodiversity and ecosystems. In addition to contributing to at least one of these objectives, sustainable investments will have to be screened to ensure they do not cause harm to any of the other objectives under the "Do not significant harm" approach, while meeting minimum social safeguards.

So far, regulatory frameworks have mainly focused on disclosure and transparency. However, supervisors are raising their expectations. In its action plan for funding sustainable growth, the European Commission [19] asserts that sustainability should be an integral part of financial institutions' risk management practices. In the banking sector, supervisors have raised their expectations in terms of the inclusion of environmental factors in credit ratings and stress testing. In its "Guide on climate and environmental-related risks: Supervisory expectations relating to risk management and disclosure," the European Central Bank [16] has set expectations, which cover specifically risk management practices.<sup>14</sup> The ECB states that "Institutions are expected to monitor, on an ongoing basis, the effect of climate-related and environmental factors on their current market risk positions and future investments, and to develop stress tests that incorporate climate-related and environmental risks." In its review published in 2021 [17], the ECB states that none of the institutions are close to fully aligning their practices with the supervisory expectations.

---

<sup>12</sup> For 2020, the Luxembourg Association for Investment Funds (ALFI) reports that 198bn Euros of net fund flows went into funds that have sustainability characteristics, out of 414bn Euros total, which represents 52% of the total (analysis based on Morningstar Direct data).

<sup>13</sup> The Taxonomy [46]/(852) on the establishment of a framework to facilitate sustainable investment was published in the Official Journal of the European Union on June 22, 2020, and entered into force on July 12, 2020. The EU taxonomy is a classification system, establishing a list of environmentally sustainable economic activities.

<sup>14</sup> Institutions are expected to incorporate climate-related and environmental risks as drivers of existing risk categories into their existing risk management framework, with a view to managing and monitoring these drivers over a sufficiently long-term horizon, and to review their arrangements on a regular basis. Institutions are expected to identify and quantify these risks within their overall process of ensuring capital adequacy. In their credit risk management, institutions are expected to consider climate-related and environmental risks at all relevant stages of the credit-granting process and to monitor the risks in their portfolios.



## 7 Opportunities for Further Integration of Nature-Related Risks

Multiple initiatives that call for enhanced approaches to address nature-related risks have emerged, both in academia and within the financial industry [8, 42, 43, 56]. The proposed frameworks address the multiple steps of a traditional risk management approach from risk identification, risk exposure measurement, to assessment and treatment.

In the first instance, they provide an opportunity to address the shortcomings in the current practices highlighted before. This includes addressing the need for enhanced disclosures and better data and improving key risk indicators and environmental risk assessment methodologies. There is also an opportunity for better integration of these risks into financial valuation and capital allocation decisions, underpinned by enhanced regulation. Furthermore, we believe that new dimensions should be integrated into the traditional risk management approach.

First, new paradigms and indicators should be applied for identification and exposure measurement. Traditionally, environmental risks have been integrated as part of the generic risk governance framework of financial institutions for risk identification and measurement. For quantitative assessments, they have been integrated as part of methods such as stress tests for capital requirements or value at-risk frameworks [5], which mainly rely on historical data. To that extent, for the banking sector, the latest European Central Bank review [17] highlights the shortcomings in terms of existing practices for environmental risk assessments and the need for specific measures to be developed and implemented.

Applying specific frameworks for assessing the financial institutions' exposure to nature-related risks could strengthen the risk identification process. Moreover, traditional bottom-up and vertical risk assessments may not be sufficient to grasp the complexity of nature-related risks. An enhanced and effective risk management approach should help to identify existing or potential interdependencies and seek to isolate risks, prevent contagion, and mitigate damage. This will also imply enhanced methods for prioritizing risks, particularly those which are longer term.

Better accounting for these risks is important, since accounting norms reflect broader worldviews of what is valued in society [30]. In terms of the actual quantification of the risks, nature-related risks may prove to be difficult to assess both in terms of likelihood and impact. As explored earlier in this chapter, many of these risks may prove to be disruptive, nonlinear, and scalable. It is thus difficult to calculate averages or risk exposures based on history. Their systemic nature also calls for system modeling and forward-looking views, such as scenario building, similar to climate risks (Bolton et al. 2021). Modeling is required to quantify our understanding of ecosystem services and to understand dynamic, nonlinear, spatially explicit trade-offs as part of the larger socioecological systems [11, 27]. In certain instances, sensitivity analysis based on simpler scenario-based risk assessments may be required for specific investments or complex projects. In addition, the long-term nature of these risks also needs to be factored in. To assess the effectiveness of a



given financial, economic, or social strategy, the observation window needs to be large enough to include substantial deviations, so one must base strategies on a long-time frame [38].

Emerging practice from the financial industry and literature point into two directions for better assessing and quantifying the potential impacts of nature-related risks. First, for dependency risks, a potential avenue for their quantification is to assign a cost to the value generated for economic activity for the service provided by the underlying ecosystem. New approaches have been emerging for quantifying ecosystem services (in addition to assessing the potential costs of natural hazards' damages). For instance, the Ecosystem Services Valuation Database (ESVD) has been launched in 2021 as the largest publicly available database and tool with standardized monetary values for all ecosystem services and all biomes on all continents ([www.esvd.info](http://www.esvd.info)). It includes several valuation methods, from replacement, restoration cost, to defensive expenditures to protect the underlying natural asset. Furthermore, the EU's biodiversity strategy [22, 23] includes further mapping and assessment of the state of the ecosystems, their services, and economic values, with the goal of incorporating their values into accounting and reporting systems at the EU national level.

The second area for better quantification of the risks is looking at their impact, focusing on the quantification of the pressures (or externalities) caused by economic activities to the environment, and assigning a cost using different valuation methods (which may, for instance, assess the cost of compensation or mitigation). This could expand on what has been done for greenhouse gases, where an implicit carbon price can be estimated, even in the absence of regulated carbon emission permits and trading systems, or without an explicit carbon tax in effect. Such an approach could be extended to better account for other nature-related pressures linked to land, water, and marine ecosystems' use, pollution, or disturbances. Several methodologies are being developed in that regard to improve biodiversity accounting approaches for businesses and financial institutions [34].

For transition risks, the likelihood or impact does not only depend on the nature and the scale of potential impacts caused by the activities, but also on the regulation, litigation, market demand, and technology costs that can occur as a result of the risk materializing with negative impacts on society. To that extent, investment practices could include further fundamental research and explicitly include the transition risk assessments [52, 53]. This might require a stark shift in risk management strategy for financial institutions. Some argue that nature-related financial risks cannot be sufficiently managed through "market fixing" approaches based on information disclosures and quantitative risk estimates [31]. They propose that financial authorities utilize a "precautionary policy approach," making greater use of qualitative methods of managing risk, to support a controlled regime shift toward more sustainable capital allocation.

In that respect, the development of "protected areas" is taking a new dimension, with targets of 30% of land and seas being covered by protected areas at the EU level in 2030 [23]. While it is not envisioned for all economic activities to completely come to a standstill in these areas, they will be severely constrained. At least a third

of the EU's protected areas will be under strict protection, including all remaining primary and old-growth forests and other carbon-rich ecosystems. The question for the financial sector then becomes whether it can effectively address the risk of exposure to these zones through its investments in geographically exposed assets. This includes new types of spatial considerations in the decision-making of financial institutions. In that respect, the EU Sustainable Finance Disclosure Regulation has led to the introduction of a new indicator (PAI 7) in 2021 [24], which is to measure the “share of investments in investee companies with sites/operations located in or near to biodiversity-sensitive areas where activities of these investee companies negatively affect these areas.”

Furthermore, financial institutions may opt for more qualitative and criteria-based approaches, which take into account nature-related risks. ESG investing can be an opportunity to engrain long termism in finance [5]. For instance, they could include higher and more minimum standards and avoid exposure to the most “at-risk” activities. In the absence of certainty and full data, these may also involve opting for precautionary approaches. When it comes to mitigating risks (i.e., reducing the extent of risk exposure and mitigating the adverse effects of risk), financial institutions are faced with the choice of risk reduction at either the level of the portfolio, or at the level of the investees or lenders. The latter implies that financial institutions have the ability to “engage” with their investees or lenders to minimize their exposure to risk by influencing their corporate governance and requesting them to raise their standards (for instance, by making it a condition as part of their loan arrangements). There is direct evidence that investors can impact companies through direct shareholder engagement, in particular when investors have influence, companies have experience with environmental issues and when the costs of requested reforms are low [33]. While they consider reducing exposures to issuers or activities that are exposed to nature-related risks, financial institutions may further invest in adaptation and transition activities. Here, one of the potential challenges to address is that the companies that invest in transition activities may be the same that carry at-risk activities, hence calling for a greater implication of the financial institutions in the capital allocation decisions within the companies they invest in or lend to.

## **8 Beyond Risk Management, an Efficient Frontier Between Precaution and Dealing with Uncertainty?**

As explored before in this chapter, one key characteristic of nature-related financial risks is their degree of uncertainty. Since Knight [32], it is common to distinguish between risk, characterized by an “objective” probability law grounded on events with a known reality and uncertainty, which does not rely on a specific basis of information due to the lack of quantifiable knowledge. As a result, it has been common to link risk to prevention and uncertainty to the principle of precaution. While prevention relates to managing risks based on current information, precaution

can also be seen as the process of managing the expectations of receiving further information and reassessing risks as knowledge progresses over time [28].

Precautionary approaches can thus have a central role to play when dealing with nature-related risks dependencies and impacts that are harder to assess and not yet fully understood. To that extent, an application of the principle of precaution for the environment in the absence of full certainty is given in principle 15 of the Rio Declaration in 1992 [57]: “*Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation.*”

A risk acceptance strategy may become rational when the cost of accepting the risk itself is lower than the cost of its mitigation. By extension, the acceptance of uncertainty can be based on the comparison between the potential threats of accepting the risk and the costs of implementing a precautionary approach. The European Commission [18] explicitly refers to this type of economic approach when it interprets the precaution principle: It stipulates that precautionary measures should be based on a review of the advantages and potential drawbacks of taking or not taking action, including when applicable to a cost–benefit analysis. In other words, one should ask whether the costs for reducing a risk are justified vis a vis the benefits they can bring. The existence of uncertainty can lead to a reduction in net benefits from an activity with environmental costs in important cases [1].

However, in certain instances, some authors argue that strong interpretations of the precautionary principle applied to environmental decisions can lead to sub-optimal outcomes, such as in the field of environmental regulation [54]. In the absence of certainty and given the challenge to quantify the risks and their inherent costs, a more targeted and explicit approach may be required for applying the principle of precaution when dealing with environmental threats. This may result in financial institutions investing and incurring mitigation costs where the nature of risks are best understood and assessed to be a source of material adverse impacts, while dealing effectively with the precaution principles in more uncertain areas.

In terms of ESG investment practices, this may translate into avoiding or mitigating exposures to investments that have potential adverse impacts, while accepting uncertainties in areas, which require transitioning toward more sustainable models. In certain case, dealing with uncertainty is certainly desirable to stimulate innovation, as long as this is complemented with swift adaptation as more knowledge is generated. In fact, innovation is critical in areas where a sustainable transition is required, such as the energy sector or the development of the circular economy.

## 9 Conclusion

The financial sector needs to engage in a review of its risk management approach toward nature-related risks. There are major nature-related impacts and dependencies embedded in the financial system that are currently not included in the risk

management approaches of the latter. Nature-related financial risks have unique characteristics and as such require dedicated attention. There are still major gaps in the current practices of financial institutions in addressing these. Moreover, for financial and economic decision-makers, treating nature-related financial risks with their traditional risk toolbox will likely not be effective.

First, there is a need to better understand nature-related risks and their impact on the financial sector and the real economy. This implies finding ways to better address their complexity and disruptive features as part of decision-making. Moreover, there is also a need for improved data, metrics, and methodologies to measure and manage these risks.

This may pave the way for further research on the most appropriate risk management practices that need to be developed. This includes research on improving the identification, assessment, and valuation of nature-related risks, allowing financial institutions to be in a better position to monitor their exposure to nature-related risks. The result of this would then push financial institutions to implement better decisions in terms of capital allocation, potentially reducing exposures to risk-exposed activities while engaging with their investees and investing in better standards and transition activities.

At the level of financial policymakers and regulators, there is an opportunity to define potential frameworks in terms of policy and prudential regulation that could also be linked to the ambition to ensure a more sustainable environment. In doing so, there is a need to go beyond simple disclosure requirements. For instance, when it comes to stress testing and prudential regulation, there have been calls for redesigning banking regulation to consider the environmental dimension of banks' riskiness as an additional component of the current prudential framework. This could, for instance, be based on the calculation and gradual implementation of pollution-based risk coefficients for capital requirements [15].

Finally, there is the opportunity of making longer-term sustainability considerations more formally integrated into the decision-making, building on changing investor awareness and preferences in terms of sustainability. Better inclusion of nature-related risks is important, since accounting norms reflect broader worldviews of what is valued in society and drive economic and financial decisions. As such, more attention to nature-related risks would ensure progress toward a more sustainable future.

## References

1. Arrow, K.J., Fisher, A.: Environmental preservation, uncertainty and irreversibility. *Q. J. Econ.* **88**(2), 312–319 (1974)
2. Barbier, E.: The concept of natural capital. *Oxf. Rev. Econ. Policy.* **35**(1), 14–36 (2019)
3. Bassen, A., Busch, T., Lopatta, K., Evans, E., Opoku, O.: Nature Risks Equal Financial Risks: A Systematic Literature Review. Universität Hamburg (2019). Available at: [https://www.wwf.ch/sites/default/files/doc-2019-11/Nature\\_Risks\\_equal\\_Financial\\_Risks\\_RG\\_Sustainable\\_Finance\\_Hamburg\\_2019\\_final.pdf](https://www.wwf.ch/sites/default/files/doc-2019-11/Nature_Risks_equal_Financial_Risks_RG_Sustainable_Finance_Hamburg_2019_final.pdf)

4. Berg, F., Koelbel, J.F., Rigobon, R., (2019) Aggregate Confusion: The Divergence of ESG Ratings. MIT Sloan Research Paper No., 5822–19
5. Bolton, P., Després, M., Pereira Da Silva, L.A., Samama, F., Svartzman, R.: The Green Swan: Central Banking and Financial Stability in the Age of Climate Change. Bank for International Settlements (BIS) and Banque de France (2020). Available at: <https://www.bis.org/publ/othp31.pdf>
6. Braat, L.C., de Groot, R.: The ecosystem services agenda: bridging the worlds of natural science and economics, conservation and development, and public and private policy. *Ecosyst. Serv.* **1**(1), 4–15 (2012)
7. Cambridge Centre for Sustainable Finance: Environmental Risk Analysis by Financial Institutions: a Review of Global Practice, 84p. Cambridge Institute for Sustainability Leadership, Cambridge (2016)
8. Cambridge Institute for Sustainability Leadership (CISL), ICBC, NCFI, UNEP FI: Enhancing Environmental Risk Assessment in Financial Decision-Making, in Support of the G20 Green Finance Study Group, July 2017. Cambridge Institute for Sustainability Leadership (2017)
9. Cambridge Centre for Sustainable Finance: Handbook for Nature-Related Financial Risks: Key Concepts and a Framework for Identification, 34p. Cambridge Centre for Sustainable Finance (2021). Available at: <https://www.cisl.cam.ac.uk/system/files/documents/handbook-for-nature-related-financial.pdf>
10. Costanza, R., d’Arge, R., de Groot, R., Farber, S., Grasso, M., Hannon, B., Limburg, K., Naeem, S., O’Neill, R.V., Paruelo, J., Raskin, R.G., Sutton, P., van den Belt, M.: The value of the world’s ecosystem services and natural capital. *Nature*. **387**, 253–260 (1997)
11. Costanza, R., de Groot, R., Braat, L., Kubiszewski, I., Fioramonti, L., Sutton, P., Farber, S., Grasso, M.: Twenty years of ecosystem services: how far have we come and how far do we still need to go? *Ecosyst. Serv.* **28-A**, 1–16 (2017)
12. Dasgupta, P.: The Economics of Biodiversity: The Dasgupta Review. HM Treasury, London (2021). Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/962785/The\\_Economics\\_of\\_Biodiversity\\_The\\_Dasgupta\\_Review\\_Full\\_Report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/962785/The_Economics_of_Biodiversity_The_Dasgupta_Review_Full_Report.pdf)
13. Diagne, C., Leroy, B., Vaissière, A.-C., Gozlan, R.E., Roiz, D., Jaric, I., Salles, J.-M., Bradshaw, C.J.A., Courchamp, F.: High and rising economic costs of biological invasions worldwide. *Nature*. **592**, 571–576 (2021)
14. Egli, F., Schärer, D., Steffen, B.: Determinants of fossil fuel divestment in European pension funds. *Ecol. Econ.* **191**, 107237 (2022)
15. Esposito, L., Mastromatteo, G., Molocchi, A.: Environment – risk-weighted assets: allowing banking supervision and green economy to meet for good. *J. Sustain. Finance Investment*. **9**(1), 68–86 (2019)
16. European Central Bank: Guide on Climate and Environmental-Related Risks. Supervisory Expectations Relating to Risk Management and Disclosure. European Central Bank (2020). Available at <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf>
17. European Central Bank: The State of Climate and Environmental Risk Management in the Banking Sector, Report on the Supervisory Review of Banks’ Approaches to Manage Climate and Environmental Risks. European Central Bank (2021). Available at: <https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202111guideonclimate-relatedandenvironmentalrisks~4b25454055.en.pdf>
18. European Commission: Communication from the Commission on the Precautionary Principle, COM(2000) 1 Final, 2.2.2000, Brussels. European Commission (2000)
19. European Commission: Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions Action Plan: Financing Sustainable Growth. European Commission (2018). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0097>

20. European Commission: Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on Sustainability-Related Disclosures in the Financial Services Sector, OJ L 317, 9.12.2019, pp. 1–16 (2019)
21. European Commission: Proposal for a Corporate Sustainability Reporting Directive, Amending Directive 2013/34/EU, Directive 2004/109/EC, Directive 2006/43/EC and Regulation (EU) No 537/2014 (2021a)
22. European Commission: Communication from the Commission to the European Parliament, the European Council, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions Action, EU Taxonomy, Corporate Sustainability Reporting, Sustainability Preferences and Fiduciary Duties: Directing finance towards the European Green Deal. Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0188&from=EN> (2021b)
23. European Commission: Directorate-General for Environment, EU Biodiversity Strategy for 2030: Bringing Nature Back into Our Lives. Available at: <https://data.europa.eu/doi/10.2779/677548> (2021c)
24. European Supervisory Authorities (ESAs): Final Report on draft Regulatory Technical Standards, with regard to the content, methodologies and presentation of sustainability-related disclosures under empowerment Articles 2a, 4(6) and (7), 8(3), 9(5), 10(2) and 11(4) of Regulation (EU) 2019/2088 (Sustainable Finance Disclosure Regulation (SFDR)) (2021)
25. Exploring Natural Capital Opportunities, Risks and Exposure (ENCORE): A Practical Guide for Financial Institutions, Natural Capital Finance Alliance and UN Environment World Conservation Monitoring Centre. Geneva, Oxford/Cambridge (2018)
26. Financial Stability Institute (FSI) of the Bank for International Settlements (BIS): Stress-Testing Banks for Climate Change – A Comparison of Practices FSI Insights on policy implementation No 34. Financial Stability Institute (FSI) of the Bank for International Settlements (BIS) (2021)
27. Fioramonti, L.: The World After GDP: Economics, Politics and International Relations in the Post-Growth Era, 240P. Polity, Cambridge (2017)
28. Gollier, C., Treich, N.: Les approches économiques de la précaution: présentation et discussion critique. *Nat. Sci. Soc.* **22**, 85–92 (2014)
29. INSPIRE & NGFS: Biodiversity and Financial Stability: Exploring the Case for Action, NGFS Occasional Paper. Available at: <https://www.ngfs.net/en/biodiversity-and-financial-stability-exploring-case-action> (2021)
30. Jourdain, E.: *Quelles Normes Comptables Pour Une Société Du Commun?* Editions Charles Léopold Mayer (2019)
31. Kedward, K., Ryan-Collins, J., Chenet, H.: *Managing Nature-Related Financial Risks: A Precautionary Policy Approach for Central Banks and Financial Supervisors.* UCL Institute for Innovation and Public Purpose Working Paper 2020-09, available at: [https://www.ucl.ac.uk/bartlett/public-purpose/sites/public-purpose/files/final\\_iipp-wp2020-09-kedward\\_et\\_al\\_nature-related\\_finance\\_edited\\_15\\_sept.pdf](https://www.ucl.ac.uk/bartlett/public-purpose/sites/public-purpose/files/final_iipp-wp2020-09-kedward_et_al_nature-related_finance_edited_15_sept.pdf) (2020)
32. Knight: *Risk, Uncertainty and Profit.* Adanson Publishing (1921)
33. Kölbel, J.F., Heeb, F., Paetzold, F., & Busch, T.: *Beyond Returns: Investigating the Social and Environmental Impact of Sustainable Investing.* Available at: <https://www.zora.uzh.ch/id/eprint/162661/1/SSRN-id3289544.pdf> (2018)
34. Lamerant, J., Müller, L., Kisielwicz, J.: *Critical Assessment of Biodiversity Accounting Approaches for Businesses and Financial Institutions.* Reports for EU Business @ Biodiversity Platform (2018/2019)
35. Lebreton, L., Egger, M., Slat, B.: A global mass budget for positively buoyant macroplastic debris in the ocean. *Sci. Rep.* **9**, 12922, 10p (2019)
36. Maas, K., Lambooy, T., Van Tilburg, R., Van't Foort, S.: *Investors and Companies' Biodiversity and Natural Capital Reporting and Performance – Assessing the Request for and Use of Company Reporting on Biodiversity and Natural Capital by Asset Managers and Fund Managers*, vol. 2017, 67p. Sustainable Finance Lab, Nyenrode Business University, Impact Centre Erasmus (2017)

37. Mandelbrot, B.B.: “New Economics,” Revisited: Short versus Long Tails and Gaussian versus Power-Law Distributions. *Complexity*. **14**(3), 55–65 (2018)
38. Mandelbrot, B., Taleb, N.N.: Mild vs. wild randomness: focusing on those risks that matter. In: Diehold, F.X., Doherty, N.A., Herring, R.J. (eds.) *The Known, the Unknown, and the Unknowable in Financial Risk Management: Measurement and Theory Advancing Practice*, pp. 47–58. De Gruyter (2010)
39. Missimer, A.: Natural capital as an economic concept, history and contemporary issues. *Ecol. Econ.* **143**, 90–96 (2018)
40. Natural Capital Coalition: Natural Capital Protocol (Online). Available at: [www.naturalcapitalcoalition.org/protocol](http://www.naturalcapitalcoalition.org/protocol), 136p (2016)
41. Natural Capital Finance Alliance (NCFA): Integrating Natural Capital in Risk Assessments: A Step-by-Step Guide for Banks, 30p. Geneva, Oxford/London (2018)
42. Network for Greening the Financial System (NGFS): NGFS Climate Scenarios for Central Banks and Supervisors, 39 p (2020a)
43. Network for Greening the Financial System (NGFS): Overview of Environmental Risk Analysis by Financial Institutions Technical Document, 55p. Network for Greening the Financial System (NGFS) (2020b)
44. OECD: Biodiversity: Finance and the Economic Business Case for Action, 124p OECD (2019)
45. Popescu, I., Claudia, H., Enrico, B.: Measuring the sustainability of investment funds: a critical review of methods and frameworks in sustainable finance. *J. Clean. Prod.* **314**, 128016 (2021)
46. Regulation (EU) 2020/852 of the European Parliament and of the Council of 18 June 2020 on the establishment of a framework to facilitate sustainable investment, and amending Regulation (EU) 2019/2088. Available at [https://ec.europa.eu/info/law/sustainable-finance-taxonomy-regulation-eu-2020-852\\_en](https://ec.europa.eu/info/law/sustainable-finance-taxonomy-regulation-eu-2020-852_en)
47. Responsible Investor and Credit Suisse: Unearthing Investor Action on Biodiversity, conducted in collaboration with The Nature Conservancy, the Zoological Society of London and the International Union for the Conservation of Nature (2021)
48. Rockström, J., Steffen, W., Noone, K., Persson, Å., Chapin III, F.S., Lambin, E., Lenton, T.M., Scheffer, M., Folke, C., Schellnhuber, H., Nykvist, B., De Wit, C.A., Hughes, T., van der Leeuw, S., Rodhe, H., Sörlin, S., Snyder, P.K., Costanza, R., Svedin, U., Falkenmark, M., Karlberg, L., Corell, R.W., Fabry, V.J., Hansen, J., Walker, B., Liverman, D., Richardson, K., Crutzen, P., Foley, J.: Planetary boundaries: exploring the safe operating space for humanity. *Ecol. Soc.* **14**(2), 32 (2009)
49. Suttor-Sorel, L., Herculim, N.: Report: Nature’s Return: Embedding Environmental Goals at the Heart of Economic and Financial Decision-making. Finance Watch, 88p. Available at [https://www.finance-watch.org/wpcontent/uploads/2020/05/Natures-Return\\_Finance-Watch-Report\\_May2020.pdf](https://www.finance-watch.org/wpcontent/uploads/2020/05/Natures-Return_Finance-Watch-Report_May2020.pdf) 68 (2020)
50. Scheibe, K.P., Blackhurst, J.: Systemic risk and the ripple effect in the supply chain. In: Ivanov, D., Dolgui, A., Sokolov, B. (eds.) *Handbook of Ripple Effects in the Supply Chain* International Series in Operations Research & Management Science, vol 276. Springer, Cham (2019)
51. Schoenmaker, D.: A Framework for Sustainable Finance, CEPR Discussion Paper, DP12603 (2018)
52. Schoenmaker, D., Schramade, W.: Principles of Sustainable Finance. Oxford University Press, Oxford (2019a)
53. Schoenmaker, D., Schramade, W.: Investing for long-term value creation. *J. Sustain. Finance Investment.* **9**(4), 356–377 (2019b)
54. Stewart, R.B.: Environmental regulatory decision making under uncertainty. In: Swanson, T. (ed.) *An Introduction to the Law and Economics of Environmental Policy: Issues in Institutional Design (Research in Law and Economics, Vol. 20)*, pp. 71–126. Emerald Group Publishing Limited, Bingley (2002)
55. Svartzman, R., Espagne, E., Gauthey, J., Hadji-Lazaro, P., Salin, M., Allen, T., Berger, J., Calas, J., Godin, A., Vallier, A.: “Silent Spring” for the Financial System? Exploring Biodiversity-Related Financial Risks in France Working Paper #826, 95p. Banque de France (2021)



56. Taskforce for Nature-related Financial Disclosures: The TNFD Nature-related Risk & Opportunity Management and Disclosure Framework. Beta v0.1 Release. A Prototype for Consultation with Market Participants March 2022 (2022)
57. United Nations Conference on Environment and Development (UNCED): Rio Declaration on Environment and Development, A/CONF.151/26 (Vol. I) (1992)
58. UN Environment Programme: Prioritising Nature-Related Disclosures. Considerations for High-Risk Sectors. UNEP-WCMC, Cambridge (2022)
59. Van Toor, J., Piljic, D., Schellekens, G., van Oorschot, M., Kok, M.: Indebted to Nature Exploring Biodiversity Risks for the Dutch Financial Sector, 44p. De Nederlandsche Bank (DNB) and Planbureau voor de Leefomgeving (PBL) (2020). Available at <https://www.pbl.nl/en/publications/indebted-to-nature>
60. Walter, C.: Sustainable financial risk modelling fitting the SDGs: some reflections. *Sustainability*. **12**(18), 7789 (2020)
61. Wassénus, E., Crona, B.I.: Adapting risk assessments for a complex future. *One Earth*. **5**(1), 35–43 (2022)
62. World Economic Forum: The Global Risks Report 2022, 17th edn. World Economic Forum (2022)
63. Wouters, J., Van Kerckhoven, S.: The EU's internal and external regulatory actions after the outbreak of the 2008 financial crisis. *Eur. Company Law*. **8**(5), 201–207 (2011)
64. WWF and PWC: Nature is Too Big to Fail. Biodiversity: The Next Frontier in Financial risk Management, Report, 40p. WWF and PWC (2020)



# Defense-Critical Supply Chain Networks and Risk Management with the Inclusion of Labor: Dynamics and Quantification of Performance and the Ranking of Nodes and Links



Anna Nagurney

## 1 Introduction

In February 2022, the U.S Department of Defense (DoD) issued a long-awaited report, “Securing Defense-Critical Supply Chains” (U.S. Department of Defense [29]). The report was in response to Executive Order (E.O.) 14017, “America’s Supply Chains,” signed by President Joseph R. Biden Jr., to identify how to improve supply chain resilience and how to protect against material shortages, which had clearly become exacerbated in the COVID-19 pandemic (see Biden Jr. [1], United States White House [28]). The DoD’s report provided an assessment of defense-critical supply chains in order to improve the department’s capacity to defend the United States. With the geopolitical risk rising globally and, with the war of Russia against Ukraine raging (cf. Bilefsky, Perez-Pena, and Nagurney and Ermagun [2]), following the major invasion, beginning February 24, 2022, having a framework for the modeling, analysis, and solution of defense-critical supply chains is of major importance. Of additional relevance is having a framework to identify which of the nodes and links, corresponding, for example, to manufacturing sites and processes, storage facilities, transportation and distribution, are important since focusing on those can help to preserve the performance of the supply chain networks for critical defense products in the case of disruptions.

Parallel to the COVID-19 pandemic, which is a global healthcare disaster, not limited in location or to a time window, the number of disasters, including “natural” disasters, has been growing as well as the people affected by them (see Nagurney and Qiang [18] and Kotsireas et al. [8]). Hence, research on supply chain network

---

A. Nagurney (✉)

Department of Operations and Information Management, Isenberg School of Management,  
University of Massachusetts, Amherst, MA, USA

e-mail: [nagurney@isenberg.umass.edu](mailto:nagurney@isenberg.umass.edu)

performance and resilience has been garnering increasing attention (see Sheffi [25], Ivanov and Dolgui [5], Nagurney and Ermagun [16], Novoszel and Wakolbinger [22], Ramakrishnan [24]), with supply chains networks for defense products being essential to national and, even global, security. In the DoD report, manufacturing, as well as the workforce, is considered to be a strategic enabler and critical to building overall supply chain resilience.

In this chapter, a defense-critical supply chain network game theory model is constructed in which the defense firms compete noncooperatively in producing, transporting, storing, and distributing their substitutable defense products, which are distinguished by firm or “brand.” Defense products could include weaponry, radars, tanks, or even life-saving vests and medical kits. The objective function faced by a defense firm that it wishes to maximize consists of the profit and the weighted total risk associated with its supply chain network. A crucial element of the model is the availability of labor associated with each supply chain network link and a bound on the labor hours available. The governing equilibrium concept is that of a Nash equilibrium [20, 21]. Under appropriate delineated assumptions, the governing equilibrium conditions are shown to satisfy a variational inequality problem for which existence of a solution is guaranteed. An alternative variational inequality is then constructed with both defense product path flows and Lagrange multipliers associated with the link labor bounds as variables, and with the underlying feasible set being the non-negative orthant. A dynamic adjustment process is then proposed utilizing the theory of projected dynamic systems (see Nagurney and Zhang [19]) and a discrete-time algorithm outlined for computational purposes. Here, we consider a defense supply chain network economy in that the defense demand markets, which can be associated with different governments, can procure the defense products from the defense firms, which can be in different countries. The supply chain network economy can correspond, for example, to defense firms associated with NATO, or the European Union, or other such organizational bodies.

We, subsequently, turn to the construction of a defense supply chain network efficiency/performance measure, which is then applied to define the importance of a network component, whether a node, a link, or a composition of nodes and links thereof. Note is then made of how the measure can be applied to measure resilience of the supply chain network to disruptions in labor. The inclusion of labor into general supply chain networks is a recent contribution and was motivated by the impacts of the COVID-19 pandemic on workers, their health, loss of productivity, etc., as well as the negative effects of shortages of labor on profits as well as consumers. Toward that end, Nagurney [12, 13] introduced labor into supply chain networks, beginning with optimization models, and then evolving to game theory models, with the model by Nagurney [14] being the most relevant to the one constructed in this chapter. Here, however, we introduce risk since risk is a characteristic of many supply chains these days due to a challenging geopolitical landscape (see also Nagurney et al. [15], Tang [26], Tang and Tomlin [27], Qiang et al. [23], Wu and Blackhurst [30], Kotsireas et al. [8]). Furthermore, defense-critical products can include high-tech elements such as computer chips, which have been

in short supply, as well as other raw materials that may be located in places under governance by antagonistic regimes.

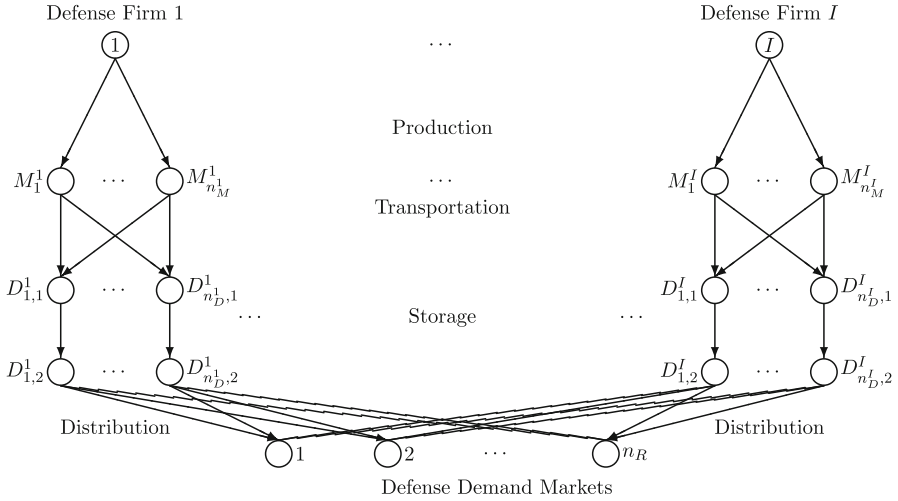
The chapter is organized as follows. In Sect. 2, the defense-critical supply chain network game theory model with labor is presented and alternative variational inequality formulations given. In addition, a dynamic version of the model is constructed, whose set of stationary points coincides with the set of solutions to the variational inequality with defense product path flows and link Lagrange multipliers associated with the labor bounds as variables. A time discretization of the continuous-time adjustment processes, in the form of a discrete algorithm, is provided. The algorithm is applied in Sect. 4 to illustrate the framework presented here in a series of defense-critical supply chain network examples. In Sect. 3, the defense supply chain network efficiency/performance measure is proposed, along with the definition of the importance of a supply chain network component. In addition, the quantification of resilience of the supply chain network to labor disruptions is highlighted. A summary of results, along with the conclusions, and suggestions for future research, is provided in Sect. 5.

## 2 Defense-Critical Supply Chain Network Game Theory Modeling

The supply chain network model with labor constructed here focuses on defense-critical products. We consider  $I$  firms involved in the production, transportation, storage, and ultimate distribution of the defense products, which are substitutable. The products could, for example, be related weaponry, such as missiles, or tanks, or even protective equipment such as helmets, life-saving vests for the military and/or citizens, or medical kits. The demand markets, here, represent the governmental defense demand markets. Note that we do not limit the model to a specific country. The demand markets can correspond to demand markets of different countries, but they are assumed to be partners and not antagonists. Hence, this model could be useful, for example, for NATO countries, for countries in the European Union, or other such coalitions.

The topology of the supply chain networks of the firms in the “defense supply chain network economy” is depicted in Fig. 1. All vectors are column vectors. The model builds upon the model in Nagurney [14] but with the addition of the crucial feature of risk management. Here, we also focus on labor bounds on links and provide, for the first time, a network performance/efficiency measure for a supply chain network game theory model with labor and a formalism for the identification of the importance of nodes and links and their ranking.

A typical defense firm is denoted by  $i$ . Each defense firm  $i$  has  $n_M^i$  production facilities; can utilize  $n_D^i$  distribution centers, and can distribute its defense product to the  $n_R$  defense demand markets.  $L^i$  represent the links of the supply chain network of defense firm  $i$ ;  $i = 1, \dots, I$ , with  $n_{L^i}$  elements. By  $G = [N, L]$  is denoted the



**Fig. 1** The defense-critical supply chain network topology

graph consisting of the set of nodes  $N$  and the set of links  $L$  in Fig. 1. The defense supply chain network topology in Fig. 1 can be modified/adapted according to the specific defense product under study.

The notation for the model is given in Table 1.

The conservation of defense product flow equations is now presented.

The demand for each defense firm's product at each defense demand market must be satisfied by the defense product flows from the defense firm to the defense demand market, as follows: For each defense firm  $i$ :  $i = 1, \dots, I$ :

$$\sum_{p \in P_k^i} x_p = d_{ik}, \quad k = 1, \dots, n_R. \quad (1)$$

Furthermore, the defense product path flows must be non-negative; where, for each defense firm  $i$ ;  $i = 1, \dots, I$ :

$$x_p \geq 0, \quad \forall p \in P^i. \quad (2)$$

The link product flows of each defense firm  $i$ ;  $i = 1, \dots, I$ , must satisfy the following equations:

$$f_a = \sum_{p \in P^i} x_p \delta_{ap}, \quad \forall a \in L^i, \quad (3)$$

where  $\delta_{ap} = 1$ , if link  $a$  is contained in path  $p$ , and 0, otherwise. Note that (3) guarantees that the flow of a defense firm's product on a link is equal to the sum of that defense product's flows on paths that contain that link.

**Table 1** Notation for the defense-critical supply chain game theory model

Notation	Definition
$P_k^i$	The set of paths in defense firm $i$ 's supply chain network ending at defense demand market $k$ ; $i = 1, \dots, I$ ; $k = 1, \dots, n_R$
$P^i$	The set of $n_{P^i}$ paths of defense firm $i$ ; $i = 1, \dots, I$
$P$	The set of $n_P$ paths in the defense supply chain network economy
$x_p$ ; $p \in P_k^i$	The non-negative flow of the defense product of firm $i$ on path $p$ originating at defense firm node $i$ and ending at defense demand market $k$ ; $i = 1, \dots, I$ ; $k = 1, \dots, n_R$ . Defense firm $i$ 's defense product path flows are grouped into the vector $x^i \in R_+^{n_{P^i}}$ . The defense firms' defense product path flows are grouped into the vector $x \in R_+^{n_P}$
$f_a$	The non-negative flow of the defense product on link $a$ , $\forall a \in L$ . The defense product link flows are grouped into the vector $f \in R_+^{n_L}$
$l_a$	The labor on link $a$ denoted in person hours, $\forall a \in L$
$\alpha_a$	Positive factor relating input of labor to output of defense product flow on link $a$ , $\forall a \in L$
$\bar{l}_a$	The upper bound on the availability of labor on link $a$ , $\forall a \in L$
$d_{ik}$	The demand for the defense product of defense firm $i$ at defense demand market $k$ ; $i = 1, \dots, I$ ; $k = 1, \dots, n_R$ . The $\{d_{ik}\}$ elements of defense firm $i$ are grouped into the vector $d^i \in R_+^{n_R}$ and all the defense product demands are grouped into the vector $d \in R_+^{In_R}$
$\hat{c}_a(f)$	The total operational cost associated with link $a$ , $\forall a \in L$
$r_a(f)$	The risk function associated with link $a$ , $\forall a \in L$
$\beta_i$	The non-negative weight applied to the evaluation of the total risk by defense firm $i$ ; $i = 1, \dots, I$ . We group all these weights into the vector $\beta$
$w_a$	The cost (wage) of a unit of labor on link $a$ , $\forall a \in L$
$\rho_{ik}(d)$	The demand price function for the defense product of defense firm $i$ at defense demand market $k$ ; $i = 1, \dots, I$ ; $k = 1, \dots, n_R$

As in Nagurney [12–14], the product output on each link is a linear function of the labor input, where

$$f_a = \alpha_a l_a, \quad \forall a \in L^i, \quad i = 1, \dots, I. \tag{4}$$

The greater the value of  $\alpha_a$ , the more productive the labor on the link. Some economic background on such a construct can be found in Mishra [9].

We also consider the following constraints on labor since shortage of skilled labor is a big issue in defense-critical supply chains: for each defense firm  $i$ ;  $i = 1, \dots, I$ :

$$l_a \leq \bar{l}_a, \quad \forall a \in L^i. \tag{5}$$

The utility function of defense firm  $i$ ,  $U^i$ ;  $i = 1, \dots, I$ , is the profit, consisting of the difference between its revenue and its total costs, the wages paid out, and the weighted total risk:

$$U^i = \sum_{k=1}^{n_R} \rho_{ik}(d) d_{ik} - \sum_{a \in L^i} \hat{c}_a(f) - \sum_{a \in L^i} w_a l_a - \beta_i \sum_{a \in L^i} r_a(f). \quad (6a)$$

The first expression after the equal sign in (6a) is the revenue of defense firm  $i$ . The second expression in (6a) is the total operational costs for the supply chain network  $L^i$  of defense firm  $i$ ; the third expression is the total payout in terms of wages to laborers of defense firm  $i$ , and the last term in (6a) is the weighted total risk of defense firm  $i$ . The utility functions  $U_i$ ;  $i = 1, \dots, I$ , are assumed to be concave, with the demand price functions being monotone decreasing and continuously differentiable and the total link cost functions being convex and also continuously differentiable with the same assumptions made for the risk functions.

Each defense firm  $i$ ;  $i = 1, \dots, I$ , hence, seeks to solve the following optimization problem:

$$\text{Maximize} \quad \sum_{k=1}^{n_R} \rho_{ik}(d) d_{ik} - \sum_{a \in L^i} \hat{c}_a(f) - \sum_{a \in L^i} w_a l_a - \beta_i \sum_{a \in L^i} r_a(f), \quad (6b)$$

subject to: (1)–(5).

We now demonstrate that the objective function of each firm  $i$ ;  $i = 1, \dots, I$ , can be expressed in path flow variables only. We proceed as follows. In view of (2) and (3), we can redefine the total operational cost link functions as:  $\tilde{c}_a(x) \equiv \hat{c}_a(f)$ ,  $\forall a \in L$ ; the demand price functions as  $\tilde{\rho}_{ik}(x) \equiv \rho_{ik}(d)$ ,  $\forall i, \forall k$ , and the risk functions  $\tilde{r}_a(x) \equiv r_a(f)$ ,  $\forall a \in L$ . As noted in Nagurney [12, 13], it follows from (3) and (4) that  $l_a = \frac{\sum_{p \in P} x_p \delta_{ap}}{\alpha_a}$ , for all  $a \in L$ .

Hence, one can redefine the utility functions  $\tilde{U}^i(x) \equiv U^i$ ;  $i = 1, \dots, I$ , and group the utilities of all the defense firms into an  $I$ -dimensional vector  $\tilde{U}$ , where

$$\tilde{U} = \tilde{U}(x). \quad (7)$$

The optimization problem faced by defense firm  $i$ ;  $i = 1, \dots, I$ , can be expressed as

$$\begin{aligned} \text{Maximize} \quad \tilde{U}^i(x) = & \sum_{k=1}^{n_R} \tilde{\rho}_{ik}(x) \sum_{p \in P_k^i} x_p - \sum_{a \in L^i} \tilde{c}_a(x) \\ & - \sum_{a \in L^i} \frac{w_a}{\alpha_a} \sum_{p \in P^i} x_p \delta_{ap} - \beta_i \sum_{a \in L^i} \tilde{r}_a(x), \end{aligned} \quad (8)$$

subject to the non-negativity constraints (1) and the re-expressing of constraints in (5) as

$$\frac{\sum_{p \in P^i} x_p \delta_{ap}}{\alpha_a} \leq \bar{l}_a, \quad \forall a \in L^i. \quad (9)$$

## 2.1 Governing Equilibrium Conditions and Variational Inequality Formulations

The governing equilibrium conditions are now stated, along with alternative variational inequality formulations.

### Nash Equilibrium Conditions and Variational Inequality Formulations

The feasible set  $K_i$  for defense firm  $i$  is defined as:  $K_i \equiv \{x^i | x^i \in R_+^{n_{pi}}, \frac{\sum_{p \in pi} x_p \delta_{ap}}{\alpha_a} \leq \bar{l}_a, \forall a \in L^i\}$ , for  $i = 1, \dots, I$ , with  $K \equiv \prod_{i=1}^I K_i$ . Clearly,  $K$  is a convex set.

Since the defense firms are utility-maximizers, they compete noncooperatively until the following Defense Supply Chain Nash Equilibrium is attained.

**Definition 1 (Defense Supply Chain Network Nash Equilibrium)** A defense product path flow pattern  $x^* \in K$  is a Defense Supply Chain Network Nash Equilibrium if for each defense firm  $i; i = 1, \dots, I$ :

$$\tilde{U}^i(x^{i*}, \hat{x}^{i*}) \geq \tilde{U}^i(x^i, \hat{x}^{i*}), \quad \forall x^i \in K_i, \tag{10}$$

where  $\hat{x}^{i*} \equiv (x^{1*}, \dots, x^{i-1*}, x^{i+1*}, \dots, x^{I*})$ .

Conditions (10) state that a Defense Supply Chain Nash Equilibrium is achieved if no defense firm can improve upon its utility unilaterally.

It follows from the classical theory of Nash equilibria and variational inequalities that, under the imposed assumptions on the total cost, the demand price, and the risk functions (cf. Gabay and Moulin [4] and Nagurney [10]), the solution to the above Defense Supply Chain Nash Equilibrium problem (see Nash [20, 21]) coincides with the solution of the variational inequality problem: Determine  $x^* \in K$ , such that

$$-\sum_{i=1}^I \langle \nabla_{x^i} \tilde{U}^i(x^*), x^i - x^{i*} \rangle \geq 0, \quad \forall x \in K, \tag{11}$$

where  $\langle \cdot, \cdot \rangle$  denotes the inner product in the corresponding Euclidean space (here, of dimension  $n_P$ ), and  $\nabla_{x^i} \tilde{U}^i(x)$  is the gradient of  $\tilde{U}^i(x)$  with respect to  $x^i$ .

Existence of a solution to variational inequality (11) is guaranteed since the feasible set  $K$  is compact and the utility functions are continuously differentiable under our imposed assumptions (cf. Kinderlehrer and Stampacchia [6]).

An alternative variational inequality to (11) is now provided over a simpler feasible set, following the arguments in Nagurney [13]. The alternative variational inequality is over the non-negative orthant and will suggest an elegant computational procedure based on the underlying dynamics as the defense firms adjust their defense product flows over time, with signals provided by Lagrange multipliers

associated with the labor link bounds, until a stationary point; equivalently, an equilibrium point satisfying the variational inequality is achieved. We associate Lagrange multipliers  $\lambda_a$  with the constraint (9) for each link  $a \in L$  and group the Lagrange multipliers for each defense firm  $i$ 's supply chain network  $L^i$  into the vector  $\lambda^i$ . All such vectors for the defense firms are then grouped into the vector  $\lambda \in R_+^{nL}$ . Also, we introduce the feasible sets:  $K_i^1 \equiv \{(x^i, \lambda^i) | (x^i, \lambda^i) \in R_+^{n_{pi} + n_{Li}}\}$ ;  $i = 1, \dots, I$ , and  $K^1 \equiv \prod_{i=1}^I K_i^1$ .

**Theorem 1 (Alternative Variational Inequality Formulation of the Defense Supply Chain Nash Equilibrium)** *The Defense Supply Chain Network Nash Equilibrium satisfying Definition 1 is equivalent to the solution of the variational inequality: determine the vector of equilibrium defense product path flows and the vector of optimal Lagrange multipliers,  $(x^*, \lambda^*) \in K^1$ , such that*

$$\begin{aligned} & \sum_{i=1}^I \sum_{k=1}^{n_R} \sum_{p \in P_k^i} \left[ \frac{\partial \tilde{C}_p(x^*)}{\partial x_p} + \beta_i \frac{\partial \tilde{R}_p(x^*)}{\partial x_p} + \sum_{a \in L^i} \frac{\lambda_a^*}{\alpha_a} \delta_{ap} + \sum_{a \in L^i} \frac{w_a}{\alpha_a} \delta_{ap} - \tilde{\rho}_{ik}(x^*) \right. \\ & \quad \left. - \sum_{l=1}^{n_R} \frac{\partial \tilde{\rho}_{il}(x^*)}{\partial x_p} \sum_{q \in P_l^i} x_q^* \right] \times [x_p - x_p^*] \\ & + \sum_{a \in L} \left[ \bar{l}_a - \frac{\sum_{p \in P} x_p^* \delta_{ap}}{\alpha_a} \right] \times [\lambda_a - \lambda_a^*] \geq 0, \quad \forall (x, \lambda) \in K^1, \end{aligned} \quad (12)$$

where

$$\frac{\partial \tilde{C}_p(x)}{\partial x_p} \equiv \sum_{a \in L^i} \sum_{b \in L^i} \frac{\partial \hat{c}_b(f)}{\partial f_a} \delta_{ap}, \quad \forall p \in P^i, \quad (13)$$

$$\frac{\partial \tilde{R}_p(x)}{\partial x_p} \equiv \sum_{a \in L^i} \sum_{b \in L^i} \frac{\partial r_b(f)}{\partial f_a} \delta_{ap}, \quad \forall p \in P^i. \quad (14)$$

**Proof** See proof of Theorem 1 in Nagurney [14].

Variational inequality (12) is now put into standard form (cf. Nagurney [10]),  $\text{VI}(F, \mathcal{K})$ , where one seeks to determine a vector  $X^* \in \mathcal{K} \subset R^{\mathcal{N}}$ , such that

$$\langle F(X^*), X - X^* \rangle \geq 0, \quad \forall X \in \mathcal{K}, \quad (15)$$

where  $F$  is a given continuous function from  $\mathcal{K}$  to  $R^{\mathcal{N}}$ ,  $\mathcal{K}$  is a given closed, convex set, and  $\langle \cdot, \cdot \rangle$  denotes the inner product in  $\mathcal{N}$ -dimensional Euclidean space.

In order to put the variational inequality (12) into the form in (15), we let  $\mathcal{N} \equiv n_P + n_L$ ;  $X \equiv (x, \lambda)$  and  $F(X) \equiv (F^1(X), F^2(X))$ , where the  $p$ th component of  $F^1(X) \equiv \frac{\partial \tilde{C}_p(x)}{\partial x_p} + \beta_i \frac{\partial \tilde{R}_p(x)}{\partial x_p} + \sum_{a \in L^i} \frac{\lambda_a}{\alpha_a} \delta_{ap} + \sum_{a \in L^i} \frac{w_a}{\alpha_a} \delta_{ap} - \tilde{\rho}_{ik}(x) - \sum_{l=1}^{n_R} \frac{\partial \tilde{\rho}_{il}(x)}{\partial x_p} \sum_{q \in P_l^i} x_q$  and the  $a$ th component of  $F^2(X) \equiv \bar{l}_a - \frac{\sum_{p \in P} x_p \delta_{ap}}{\alpha_a}$ .



## 2.2 Dynamics and Algorithm

It is interesting and valuable to also discuss the underlying dynamics as the defense firms adjust their defense product outputs over time and the Lagrange multipliers associated with the link labor bounds also evolve over time. For this purpose, we can apply the theory of projected dynamical systems (cf. Dupuis and Nagurney [3] and Nagurney and Zhang [19]). We recall the projection operator  $\Pi_{\mathcal{K}}(X, v)$ :

$$\Pi_{\mathcal{K}}(X, v) = \lim_{\delta \rightarrow 0} \frac{(P_{\mathcal{K}}(X + \delta v) - X)}{\delta}, \quad (16)$$

with  $P_{\mathcal{K}}$  being the classical projection operator (see Nagurney [10]). The ordinary differential equation of interest is then

$$\dot{X} = \Pi_{\mathcal{K}}(X, -F(X)), \quad X(0) = X^0 \in \mathcal{K}. \quad (17)$$

We know from Theorem 1.23 in Nagurney [10] that a stationary point  $X^*$  of the projected dynamical system (17), which, by definition, satisfies

$$0 = \Pi_{\mathcal{K}}(X^*, -F(X^*)), \quad (18)$$

coincides with the solution of variational inequality (15).

Specifically, in the context of the model, the rate of change of the defense product flow at a point in time on a path  $p$  depends on  $-\frac{\partial C_p(x)}{\partial x_p} - \beta_i \frac{\partial \bar{R}_p(x)}{\partial x_p} - \sum_{a \in L^i} \frac{\lambda_a}{\alpha_a} \delta_{ap} - \sum_{a \in L^i} \frac{w_a}{\alpha_a} \delta_{ap} + \tilde{\rho}_{ik}(x) + \sum_{l=1}^{n_R} \frac{\partial \tilde{\rho}_{il}(x)}{\partial x_p} \sum_{q \in P_l^i} x_q$  at that point in time, whereas the rate of change of the Lagrange multiplier on a link  $a$  depends on  $-\bar{l}_a + \frac{\sum_{p \in P} x_p \delta_{ap}}{\alpha_a}$  at the point in time. If the marginal revenue associated with a path of a firm's supply chain network exceeds the marginal costs plus the weighted marginal risk on the path, then the defense product flow will increase; if not, it will decrease, provided that it does not become negative. The projection operator  $\Pi_{\mathcal{K}}$  guarantees that the evolution of the product path flows and of the Lagrange multipliers always lies within the feasible set  $\mathcal{K}$ ; in other words, they always remain non-negative. A plethora of dynamic supply chain network models, including multitiered ones (but without labor), can be found in the book by Nagurney [11]. Nagurney and Ermagun [16] used the modified projection method of Korpelevich [7], whereas in this chapter, the Euler method is used.

Observe that (17) represents a continuous-time adjustment process. However, for computational purposes, a discrete-time algorithm that can be easily implemented is needed. For the solution of the model, we propose the Euler method, which is induced by the general iterative scheme of Dupuis and Nagurney [3], with its statement being as follows.

### The Euler Method

Initialize with  $X^0 \in \mathcal{K}$  and set  $\tau = 0$ . Compute

$$X^{\tau+1} = P_{\mathcal{K}}(X^{\tau} - a_{\tau} F(X^{\tau})), \quad (19)$$

where  $\sum_{\tau=0}^{\infty} a_{\tau} = \infty$ ,  $a_{\tau} > 0$ ,  $a_{\tau} \rightarrow \infty$ , as  $\tau \rightarrow \infty$ .

As mentioned earlier, the feasible set  $\mathcal{K}$  for the variational inequality (12) (see also 15) for the defense supply chain network model is the non-negative orthant, and, hence, the resolution of the algorithmic scheme in (19) yields closed-form expressions for the defense product path flows and for the Lagrange multipliers as stated below.

### Explicit Formulae for the Defense Product Path Flows at an Iteration

At iteration  $\tau + 1$ , one computes the following for each path  $p$ ;  $p \in P_k^i$ ,  $\forall i, k$ :

$$x_p^{\tau+1} = \max \left\{ 0, x_a^{\tau} - a_{\tau} \left( \frac{\partial \tilde{C}_p(x^{\tau})}{\partial x_p} + \beta_i \frac{\partial \tilde{R}_p(x^{\tau})}{\partial x_p} + \sum_{a \in L^i} \frac{\lambda_a^{\tau}}{\alpha_a} \delta_{ap} + \sum_{a \in L^i} \frac{w_a}{\alpha_a} \delta_{ap} - \tilde{\rho}_{ik}(x^{\tau}) - \sum_{l=1}^{n_R} \frac{\partial \tilde{\rho}_{il}(x^{\tau})}{\partial x_p} \sum_{q \in P_l^i} x_q^{\tau} \right) \right\}; \quad (20)$$

### Explicit Formulae for the Lagrange Multipliers at an Iteration

At iteration  $\tau + 1$ , one computes the following for each Lagrange multiplier  $a \in L$ :

$$l_a^{\tau+1} = \max \left\{ 0, l_a^{\tau} - a_{\tau} \left( \bar{l}_a - \frac{\sum_{p \in P} x_p^{\tau} \delta_{ap}}{\alpha_a} \right) \right\}. \quad (21)$$

We apply this algorithm in Sect. 4 to defense supply chain network examples for which we report the solutions, along with the network performance/efficiency values and additional information, using also results in Sect. 3.

## 3 Defense Supply Chain Network Efficiency/Performance

It is important to recognize that, in matters of defense, a government, in preparing for conflicts and/or in times of war, may need to acquire defense supplies from a country other than its own. Our defense supply chain network model allows for this, and we see that this is happening now as the war by Russia against Ukraine rages. Hence, we believe that an adaptation of the constructs for supply chain network performance/efficiency of Nagurney and Qiang [18] and of Nagurney and Li [17] can also be applied to the new model in this chapter, with note that the new model, unlike the previous ones in the above citations, includes labor; plus, we also have explicit weighted risk functions since risk is of high relevance in the defense sector.

### 3.1 *Efficiency/Performance of a Defense Supply Chain Network and Importance Identification of a Network Component*

The efficiency/performance of a defense supply chain network, denoted by *efficiency*,  $\mathcal{E}$ , is defined as

$$\mathcal{E} = \mathcal{E}(G, \hat{c}, \rho, w, r, \beta, \alpha, \bar{l}) \equiv \sum_{i=1}^I \sum_{k=1}^{n_R} \frac{d_{ik}^*}{In_R}, \tag{22}$$

with the demands,  $d^*$ , and the incurred defense demand market prices in (22), evaluated at the solution to (12). Observe that, given a defense supply chain network economy, and the various parameters and functions, the corresponding multifirm supply chain network is considered as performing better if, on the average, it can handle higher demands at lower prices. Note that, as can be inferred from variational inequality (12), the defense demand market prices capture the information associated with the operational costs, the wages paid out to labor, as well as the weighted risk.

Following then Nagurney and Qiang [18] for results therein for supply chains and Nagurney and Li [17], one can then define the importance of a component  $g$  (node, link, or a combination of nodes and links),  $I(g)$ , which represents the efficiency drop when  $g$  is removed from the defense supply chain network, as

$$I(g) = \frac{\Delta \mathcal{E}}{\mathcal{E}} = \frac{\mathcal{E}(G, \hat{c}, \rho, w, r, \beta, \alpha, \bar{l}) - \mathcal{E}(G - g, \hat{c}, \rho, w, r, \beta, \alpha, \bar{l})}{\mathcal{E}(G, \hat{c}, \rho, w, r, \beta, \alpha, \bar{l})}. \tag{23}$$

One can rank the importance of nodes or links, using (23). This formalism can be quite valuable for those engaged in decision-making and policymaking in the military and defense. Those defense supply chain network components that are of higher importance should be paid greater attention to since a disruption to those components will have a bigger overall impact.

Using the above efficiency/performance measure  $\mathcal{E}$ , one can also quantify the resilience of the defense supply chain network economy to disruptions in labor as discussed in Nagurney and Ermagun [16], but in the context of a supply chain network optimization model with labor and not a game theory model that also captures risk.

### 3.2 *Resilience Measure Associated with Labor Disruptions*

We can adapt the measure proposed in Nagurney and Ermagun [16] for the defense supply chain network game theory model. As therein, let  $\bar{l}_\gamma$  denote the reduction of

labor availability with  $\gamma \in (0, 1]$  so if  $\gamma = 0.8$  this means that the labor availability associated with the labor constraints is now 80% of the original labor availability as in  $\mathcal{E}$ .

### Resilience Measure Capturing Labor Availability

One can define the resilience measure with respect to labor availability,  $\mathcal{R}^{\bar{l}\gamma}$ , as

$$\mathcal{R}^{\bar{l}\gamma} \equiv \bar{\mathcal{R}}^{\bar{l}\gamma}(G, \hat{c}, \rho, \pi, \alpha, \bar{l}) = \frac{\mathcal{E}^{\bar{l}\gamma}}{\mathcal{E}} \times 100\%, \quad (24)$$

with  $\mathcal{E}$  as in (22).

The expression (24) quantifies the resilience of the defense supply chain network subject to reduction of labor availability. The closer the value is to 100%, the greater the resilience.

## 4 Numerical Examples

In this section, the modeling framework is illustrated through numerical examples. The Euler method was implemented in FORTRAN and a Linux system used for the computations. The  $\{a_\tau\}$  sequence used was  $\{10(1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \dots)\}$ . The algorithm was initialized with a demand of 40 for each demand market of each firm with the demand equally distributed among the paths of each firm. The initial Lagrange multipliers were set to 0.00. The algorithm was deemed to have converged when the absolute value of each computed variable evaluated at two successive iterations differed by no more than  $10^{-7}$ .

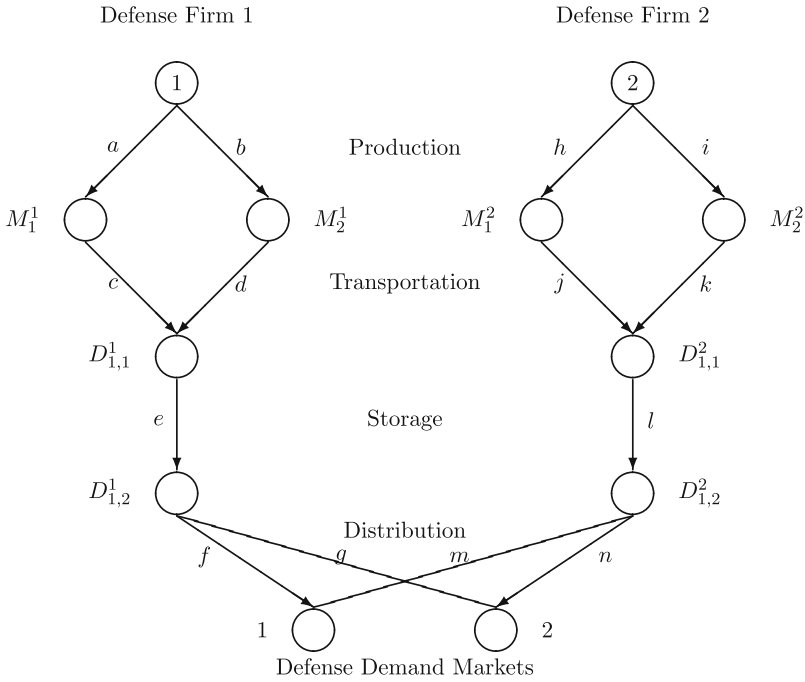
The defense supply chain network economy for the specific defense product, which could correspond, for example, to helmets or protective vests, consists of two defense firms, each of which has two production sites, a single distribution center, and serves two defense demand markets, as depicted in Fig. 2.

**Example 1 (Baseline)** The first example, which serves as the baseline, has the following data. Note that, in this example, we assume that the firms are not concerned about risk, so that all the risk functions are identically equal to 0.00.

The total operational cost functions associated with Defense Firm 1's supply chain network links  $L^1$  are

$$\begin{aligned} \hat{c}_a(f) &= 0.006f_a^2, & \hat{c}_b(f) &= 0.007f_b^2, & \hat{c}_c(f) &= 0.01f_c^2, & \hat{c}_d(f) &= 0.01f_d^2, \\ \hat{c}_e(f) &= 0.02f_e^2, & \hat{c}_f(f) &= 0.05f_f^2, & \hat{c}_g(f) &= 0.05f_g^2. \end{aligned}$$

The total operational costs associated with Defense Firm 2's supply chain network links  $L^2$  are



**Fig. 2** The supply chain network topology for the numerical examples

$$\hat{c}_h(f) = 0.0075 f_h^2, \quad \hat{c}_i(f) = 0.008 f_i^2, \quad \hat{c}_j(f) = 0.005 f_j^2, \quad \hat{c}_k(f) = 0.005 f_k^2,$$

$$\hat{c}_l(f) = 0.015 f_l^2, \quad \hat{c}_m(f) = 0.1 f_m^2, \quad \hat{c}_n(f) = 0.1 f_n^2.$$

The hourly labor wages are

$$w_a = 10, \quad w_b = 10, \quad w_c = 15, \quad w_d = 15, \quad w_e = 20, \quad w_f = 17, \quad w_g = 18,$$

$$w_h = 11, \quad w_i = 22, \quad w_j = 15, \quad w_k = 15, \quad w_l = 18, \quad w_m = 18, \quad w_n = 18.$$

The link labor productivity factors are

$$\alpha_a = 24, \quad \alpha_b = 25, \quad \alpha_c = 100, \quad \alpha_d = 100, \quad \alpha_e = 50, \quad \alpha_f = 100, \quad \alpha_g = 100,$$

$$\alpha_h = 23, \quad \alpha_i = 24, \quad \alpha_j = 100, \quad \alpha_k = 100, \quad \alpha_l = 70, \quad \alpha_m = 100, \quad \alpha_n = 100.$$

The bounds on labor are

$$\bar{l}_a = 100, \quad \bar{l}_b = 200, \quad \bar{l}_c = 300, \quad \bar{l}_d = 300, \quad \bar{l}_e = 100, \quad \bar{l}_f = 120, \quad \bar{l}_g = 120,$$

$$\bar{l}_h = 800, \quad \bar{l}_i = 90, \quad \bar{l}_j = 200, \quad \bar{l}_k = 200, \quad \bar{l}_l = 300, \quad \bar{l}_m = 100, \quad \bar{l}_n = 100.$$

The demand price functions of Defense Firm 1 are

$$\rho_{11}(d) = -0.0001d_{11} - 0.00005d_{21} + 600, \quad \rho_{12}(d) = -0.0002d_{12} - 0.0001d_{22} + 800.$$

The demand price functions of Defense Firm 2 are

$$\rho_{21}(d) = -0.0003d_{21} + 700, \quad \rho_{22}(d) = -0.0002d_{22} + 700.$$

The paths are  $p_1 = (a, c, e, f)$ ,  $p_2 = (b, d, e, f)$ ,  $p_3 = (a, c, e, g)$ ,  $p_r = (b, d, e, g)$  for Defense Firm 1 and  $p_5 = (h, j, l, m)$ ,  $p_6 = (i, k, l, m)$ ,  $p_7 = (h, j, l, n)$ , and  $p_8 = (i, k, l, n)$  for Defense Firm 2.

The computed equilibrium defense product path flows are reported in Table 2. The computed equilibrium labor values are reported in Table 3. All the Lagrange multipliers have a value of 0.00 at the equilibrium.

The defense product prices at equilibrium are

$$\rho_{11} = 599.75, \quad \rho_{12} = 799.10, \quad \rho_{21} = 699.40, \quad \rho_{22} = 699.60,$$

with the equilibrium demands:

$$d_{11}^* = 1506.19, \quad d_{12}^* = 3494.12, \quad d_{21}^* = 1999.04, \quad d_{22}^* = 2001.03.$$

The utility for Defense Firm 1 is 2,258,772.50 and that for Defense Firm 2 is 1,649,827.75.

We report the efficiency of this supply chain network, even with all the risk functions set to 0.00. The  $\mathcal{E} = 3.15$ .

**Table 2** Equilibrium defense product path flows for Examples 1 and 2

Equilibrium product path flows	Ex. 1	Ex. 2
$x_{p_1}^*$	703.17	0.00
$x_{p_2}^*$	803.02	0.00
$x_{p_3}^*$	1696.82	345.41
$x_{p_4}^*$	1797.30	345.08
$x_{p_5}^*$	919.52	152.84
$x_{p_6}^*$	1079.51	152.66
$x_{p_7}^*$	920.51	152.99
$x_{p_8}^*$	1080.52	152.81

**Table 3** Equilibrium link labor values for Examples 1 and 2

Equilibrium link labor values	Ex. 1	Ex. 2
$l_a^*$	100.00	14.39
$l_b^*$	104.01	13.80
$l_c^*$	24.00	3.45
$l_d^*$	26.00	3.45
$l_e^*$	100.00	13.81
$l_f^*$	15.06	0.00
$l_g^*$	34.94	6.90
$l_h^*$	80.00	13.30
$l_i^*$	90.00	12.73
$l_j^*$	18.40	3.06
$l_k^*$	21.60	3.05
$l_l^*$	57.14	8.73
$l_m^*$	19.99	3.05
$l_n^*$	20.01	3.96

**Example 2 (Addition of Risk Functions Associated with Production Sites)**  
 Example 2 has the same data as that in Example 1, except that now we consider the situation that the production sites are suffering from geopolitical risk and, hence, we have

$$r_a = f_a^2, \quad r_b(f) = f_b^2, \quad r_h(f) = f_h^2, \quad r_i(f) = f_i^2,$$

with the risk weights of the two firms:  $\beta_1 = \beta_2 = 1$ .

The computed equilibrium path flows are reported in Table 2, with the computed labor values given in Table 3. All the Lagrange multipliers, again, have a value of 0.00 at the equilibrium. In other words, the respective labor bounds are not reached in Example 2.

The defense product prices at equilibrium are now

$$\rho_{11} = 599.98, \quad \rho_{12} = 799.83, \quad \rho_{21} = 699.91, \quad \rho_{22} = 699.94,$$

with the equilibrium demands:

$$d_{11}^* = 0.00, \quad d_{12}^* = 690.49, \quad d_{21}^* = 305.50, \quad d_{22}^* = 305.80.$$

The utility for Defense Firm 1 now is 275,793.59 and that for Defense Firm 2: 213,562.31. One can see that the utilities of both firms have dropped precipitously in comparison to the utilities that they earned in Example 1, when there was no risk. The efficiency of this defense supply chain network, with risk functions associated with production sites,  $\mathcal{E} = 0.43$ . We see that this value is much lower than that in Example 1. We then proceeded to see how resilient this defense supply chain network is with respect to labor disruptions. We calculated  $\mathcal{R}^{\bar{I}\gamma}$  for

**Table 4** Efficiency of the defense supply chain network for Example 2 when Link  $g$  is removed and the importance  $I(g)$

$g$	$\mathcal{E}(G - g)$	$I(g)$
$a$	2.43	-4.43
$b$	0.90	-1.08
$c$	0.89	-1.08
$d$	0.89	-1.08
$e$	0.77	-0.79
$f$	1.01	-1.39
$g$	0.99	-1.30
$h$	0.99	-1.30
$i$	0.34	0.21
$j$	0.34	0.21
$k$	0.34	0.21
$l$	0.22	0.50
$m$	0.46	-0.06
$n$	0.42	0.03

$\gamma = 0.9, 0.7, 0.5, 0.3, 0.1$  and found that  $\mathcal{R}^{\bar{l}\gamma} = 1$  for all the values of  $\gamma$  noted, except when  $\gamma = 0.1$ , where  $\mathcal{R}^{\bar{l}.1} = 0.7$ . We can conclude that this defense supply chain network, with the data provided, is quite resilient to labor disruptions.

In Table 4, we report the efficiency of the defense supply chain network for Example 2 when a link  $g$  is removed, along with the importance  $I(g)$ , for  $g = a, \dots, n$ . Table 4 provides interesting results. Overall, one can see that the supply chain network of Defense Firm 2 is more important than that of Defense Firm 1 to this defense supply chain network economy, and cognizant governments should make note of this. Indeed, five of the seven links of Defense Firm 2's supply chain network have positive values in terms of their importance. Furthermore, Defense Firm 2's link  $l$ , which corresponds to a storage link, has the highest importance value; therefore, every effort should be expended to preserve its functionality. Also, the production link  $i$  of Defense Firm 2 merits maintenance and care as do the transportation links  $j$  and  $k$ . Finally, link  $m$ , a distribution link to Defense Demand Market 2, is also of importance. As for the supply chain network of Defense Firm 1, link  $e$ , which is a storage link, has the highest value in terms of importance for Defense Firm 1 and, interestingly, its production site associated with link  $a$  is of the lowest importance. We emphasize that not only the absolute values in terms of importance of supply chain network components are relevant but also their relative values.



## 5 Summary, Conclusions, and Suggestions for Future Research

In this chapter, a defense-critical supply chain network game theory model was introduced, which includes labor and associated constraints, as well as risk, since current world events have heightened the importance of both risk management and resilience of supply chain networks to disruptions, including those associated with labor, which have been significant in the COVID-19 pandemic. The methodological framework for the modeling, analysis, and computations made use of both variational inequality theory and the theory of projected dynamical systems.

We proposed a noncooperative game theory model consisting of defense firms seeking to supply defense products that are substitutable to demand markets, which can be associated with different governments that are not antagonistic to one another. The labor constraints are bounds on hours of labor available on the supply chain network links, which are production, transportation, storage, and distribution links. The utility function of each firm captures revenue as well as weighted risk and the governing equilibrium concept is that of a Nash equilibrium. Under appropriate assumptions on the utility functions, we provide alternative variational inequality formulations of the governing equilibrium conditions. In addition, a dynamic model is constructed, whose stationary points coincide with the set of solutions to the variational inequality with variables consisting of defense product path flows and Lagrange multipliers associated with the labor constraints. An algorithm, the Euler method, is proposed for the time discretization of the continuous-time trajectories and used in the solution of the numerical examples.

In addition, a network efficiency/performance measure is proposed for the defense supply chain network economy, which can then be applied to quantify the importance of supply chain network components, and then rank them. A resilience measure is also constructed to assess the impacts of disruptions to labor availability.

In order to illustrate the defense supply chain network modeling framework, numerical examples are solved with input and output data reported. The information regarding the defense supply chain network economy, made possible with the tools in the chapter, can be useful for decision-makers and policymakers in governments that are concerned about defense.

It would be interesting, for future research, to investigate the supply chain network efficiency under different kinds of labor constraints (see also Nagurney [14]) and also under different productivity levels (Nagurney and Ermagun [16]). It would also be worthwhile to include additional tiers in the supply chain network to include, specifically, suppliers and their behavior, along with labor, and address issues of supply chain network efficiency and resilience in the defense sector.

**Acknowledgments** This chapter is dedicated to the Ukrainians fighting for the freedom of their country and to the memory of all those who have lost their lives and who are suffering in Russia's war against Ukraine.

## References

1. Biden, J., Jr.: Executive Order on America's supply chains (2021). February 24, Washington DC; Available at: <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>
2. Bilefsky, D., Perez-Pena, R., Nagurney, E.: The roots of the Ukraine war: How the crisis developed (2022). The New York Times, April 21; Available at: <https://www.nytimes.com/article/russia-ukraine-nato-europe.html>
3. Dupuis, P., Nagurney, A.: Dynamical systems and variational inequalities. *Ann. Oper. Res.* **44**, 7–42 (1993)
4. Gabay, D., Moulin, H.: On the uniqueness and stability of Nash equilibria in noncooperative games. In: Bensoussan, A., Kleindorfer, P., Tapiero, C.S. (eds.), *Applied Stochastic Control of Econometrics and Management Science*, pp. 271–294. North-Holland, Amsterdam, The Netherlands (1980)
5. Ivanov, D., Dolgui, A.: Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *Int. J. Prod. Res.* **58**(10), 2904–2915 (2020)
6. Kinderlehrer, D., Stampacchia, G.: *An Introduction to Variational Inequalities and Their Applications*. Academic Press, New York (1980)
7. Korpelevich, G.M.: The extragradient method for finding saddle points and other problems. *Matekon* **13**, 35–49 (1977)
8. Kotsireas, I.S., Nagurney, A., Pardalos, P.M., Tsokas, A., (eds.): *Dynamics of Disasters: Impact, Risk, Resilience, and Solutions*. Springer International Publishing, Switzerland (2021)
9. Mishra, S.K.: A brief history of production functions (2007). MPRA Paper No. 5254. <http://mpra.ub.uni-muenchen.de/5254/>
10. Nagurney, A.: *Network Economics: A Variational Inequality Approach*, 2nd and revised edition. Kluwer Academic Publishers, Boston, MA (1999)
11. Nagurney, A.: *Supply Chain Network Economics: Dynamics of Prices, Flows, and Profits*. Edward Elgar Publishing, Cheltenham, UK (2006)
12. Nagurney, A.: Perishable food supply chain networks with labor in the Covid-19 pandemic. In: I.S. Kotsireas, A. Nagurney, P.M. Pardalos, A. Tsokas, (eds.), *Dynamics of Disasters - Impact, Risk, Resilience, and Solutions*, pp 173–193. Springer Nature Switzerland AG (2021a)
13. Nagurney, A.: Optimization of supply chain networks with the inclusion of labor: Applications to Covid-19 pandemic disruptions. *Int. J. Prod. Econ.* **235**, 108080 (2021b)
14. Nagurney, A.: Supply chain game theory network modeling under labor constraints: Applications to the Covid-19 pandemic. *Eur. J. Oper. Res.* **293**(3), 880–891 (2021c)
15. Nagurney, A., Cruz, J., Dong, J., Zhang D.: Supply chain networks, electronic commerce, and supply side and demand side risk. *Eur. J. Oper. Res.* **164**(1), 120–142 (2005)
16. Nagurney, A., Ermagun, A.: Resilience of supply chain networks to labor disruptions (2022). Resilience Findings, June 16
17. Nagurney, A., Li, D.: *Competing on Supply Chain Quality: A Network Economics Perspective*. Springer International Publishing, Switzerland (2016)
18. Nagurney, A. Qiang, Q.: *Fragile Networks: Identifying Vulnerabilities and Synergies in an Uncertain World*. Wiley, Hoboken, NJ (2009)
19. Nagurney, A., Zhang, D.: *Projected Dynamical Systems and Variational Inequalities with Applications*. Kluwer Academic Publishers, Norwell, MA (1996)
20. Nash, J.F.: Equilibrium points in n-person games. *Proc. Natl. Acad. Sci. USA* **36**, 48–49 (1950)
21. Nash, J.F.: Noncooperative games. *Ann. Math.* **54**, 286–298 (1951)
22. Novoszel, L., Wakolbinger, T.: Meta-analysis of supply chain disruption research. *Oper. Res. Forum* **3**(1), 1–25 (2022)

23. Qiang, Q., Nagurney, A., Dong, J.: Modeling of supply chain risk under disruptions with performance measurement and robustness analysis. In: T. Wu, J. Blackhurst, (eds.), *Managing Supply Chain Risk and Vulnerability: Tools and Methods for Supply Chain Decision Makers*, pp. 91–111. Springer, Berlin, Germany (2009)
24. Ramakrishnan, Y., (ed.): *Handbook of Research on Supply Chain Resiliency, Efficiency, and Visibility in the Post-Pandemic Era*. IGI Global, Hershey, PA (2022)
25. Sheffi, Y.: *The Power of Resilience: How the Best Companies Manage the Unexpected*. MIT Press, Cambridge, MA (2015)
26. Tang, C.S.: Robust strategies for mitigating supply chain disruptions. *Int. J. Logist. Res. Appl.* **9**(1), 33–45 (2006). <https://doi.org/10.1080/13675560500405584>
27. Tang, C., Tomlin, B.: The power of flexibility for mitigating supply chain risks. *Int. J. Prod. Econ.* **116**(1), 12–27 (2008)
28. United States White House: Building resilient supply chains, Revitalizing American manufacturing, and fostering broad-based growth, 100-Day Reviews Under Executive Order 14017 (2021). Washington DC, June
29. U.S. Department of Defense: Securing defense-critical supply chains (2022). Washington, DC, February; Available at: <https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF>
30. Wu, T., Blackhurst, J., (eds.): *Managing Supply Chain Risk and Vulnerability: Tools and Methods for Supply Chain Decision Makers*. Springer, Berlin, Germany (2009)

# Facing Shortages: Practical Strategies to Improve Supply Chain Resilience



Dimitra Kalaitzi  and Naoum Tsolakis 

## 1 Introduction

Risks impact the performance of firms' operations, propagate, and negatively affect end-to-end supply chain networks. Nowadays, global supply chains are exposed to a multitude of low-probability high-impact disruptive events, thus necessitating rethinking strategies to ensure agility, adaptability, and stakeholders' alignment to respond and prepare for future shocks [17]. Three main supply chain risk categories are recognized according to their origin, namely (1) internal to the firm; (2) external to the firm (i.e., supply and demand risks); and (3) environmental risks [14].

Supply risks (i.e., material flow interruptions upstream of a supply network) are common, emerging due to diverse geopolitical and public health factors, e.g., the COVID-19 pandemic and Brexit. For example, van Hoek [61] highlighted shortages in supplies due to mobility restrictions imposed as a measure against the spread of the COVID-19 pandemic; the author stressed the need to build redundancy, diversity, and resilience in the post-pandemic period. In 2021, the automotive and electronic industries experienced severe chip shortages due to COVID-19 pandemic-induced manufacturing disruptions and delivery delays combined with surged demand for electronic technologies [6], accentuated by additional supply network interruptions (e.g., Suez Canal blockage). To this effect, several companies

---

D. Kalaitzi (✉)

Department of Engineering Systems & Supply Chain Management, College of Engineering and Physical Sciences, Aston University, Aston Triangle, Birmingham, UK  
e-mail: [d.kalaitzi3@aston.ac.uk](mailto:d.kalaitzi3@aston.ac.uk)

N. Tsolakis

Department of Supply Chain Management, School of Economics and Business Administration, International Hellenic University, Thessaloniki, Greece  
e-mail: [ntsolakis@ihu.gr](mailto:ntsolakis@ihu.gr)

halted their manufacturing operations or could not fulfill customer demand (e.g., Ford Motor, General Motors, and Toyota). Contemporarily, another threat to the global supply chain and logistics sector was the limited workforce availability [46]. This latter issue was more apparent in the UK due to Brexit, which led to shortages in truck drivers.

Natural resource scarcity is another significant risk in supply chains [36]. Over the past decades, the scarcity of natural resources has had a prominent position on public policy and corporate agendas. Nations are trying to implement certain practices to secure the needed natural resources to keep operations running smoothly and achieve economic growth. For example, there is a shortage of rare earth metals such as lithium, nickel, cobalt, and manganese, and the current supply of these materials cannot meet battery demand in 2030 [69]. Another recent example refers to China's energy supply shortage that led suppliers of leading companies such as Apple and Tesla to suspend manufacturing production. Thus, organizations need to secure access to critical resources and minimize disruptions to ensure the uninterrupted flow of people, material, and production equipment.

Based on many emerging threats, it is crucial to achieve supply chain resilience, identify strategies to minimize the impact of supply chain disruptions, and enable supply networks to recover to the initial or even better functional state [33]. While the extant literature has begun to synthesize these various concepts, there has not been, to date, a systematic review of how these concepts relate to resource shortages and scarcity in the fields of supply chain management and logistics. This research aims to investigate the existing literature to (i) identify the resources that have been indicated as scarce and the causes of the shortages and (ii) propose practical strategies to build supply chain resilience.

The study is organized as follows: Sect. 2 describes the methodology used for analyzing the extant literature. Section 3 presents the study findings, including a descriptive analysis of the reviewed papers, and inserts critical taxonomies on resource shortages causes and pertinent mitigation strategies. Section 4 discusses the study findings and observations, provides key recommendations, and proposes a conceptual framework that shows the linkages between scarce resources and practical management strategies.

## 2 Research Methodology

In order to develop a coherent conceptual structure and a firm foundation of resource shortages and practical strategies to improve supply chain resilience, the extant literature was used as the object of scrutiny in this study [64, 65], and the subsequent steps were followed [20]: (i) formulation of the research question (this step is completed in the introductory section of this chapter); (ii) identification of relevant research studies; (iii) selection and evaluation of the retrieved works; (iv) critical analysis and synthesis of the findings; and (v) presentation of the results. These

steps ensure that the research methodology process is transparent, auditable, and replicable.

## ***2.1 Search Strategy and Inclusion Criteria***

Three academic databases, namely EBSCO, Scopus, Web of Science, and Google Scholar databases, were used to identify scientific articles in the extant literature. The following keyword search queries were used, namely as follows:

- “supply chain management” OR “supply” AND “shortage”
- “supply chain” OR “supply” AND “natural resource scarcity”
- “procurement” OR “purchasing” AND “shortage”
- “procurement” OR “purchasing” AND “natural resource scarcity”

The terms were searched in the title, abstract, or keywords fields, and no specific timeframe was set for the literature search. Furthermore, except for published academic papers, we also considered conference and industrial and practice-oriented papers [59]. According to Garousi et al. [24], grey literature (i.e., preprints, e-prints, technical reports, lecture notes, and Web documents from intergovernmental and nongovernmental organizations) can significantly contribute to a comprehensive review. Moreover, the reviewed publications were written in English.

## ***2.2 Studies’ Selection and Evaluation***

The retrieved articles were screened by investigating the titles and abstracts. Studies were accepted if they met the inclusion criteria, focused on resource shortages and scarcity issues in supply chains, and emphasized relevant mitigation strategies to achieve resilience. In total, 250 relevant records were identified, and after eliminating the duplicated studies and screening the articles based on titles and abstracts, 44 studies remained. Ultimately, following a thorough review, only 38 articles were deemed relevant to this study. Figure 1 depicts the review methodology process flow.

## ***2.3 Analysis and Critical Taxonomy***

Zhong et al. [70] highlighted a need to describe the main research themes and topics within selected articles. In this vein, the following research methodology step was to analyze and taxonomize the relevant secondary data. First, the VOSviewer (<https://www.vosviewer.com>) software tool was used to conduct a bibliometric analysis of the reviewed articles. Specifically, a text mining analysis was performed on the

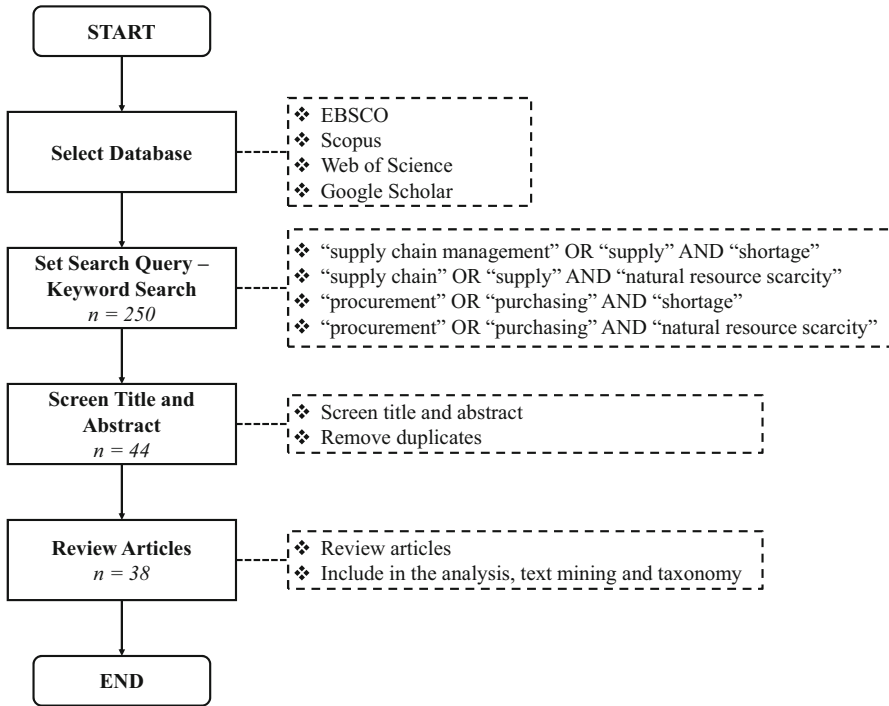


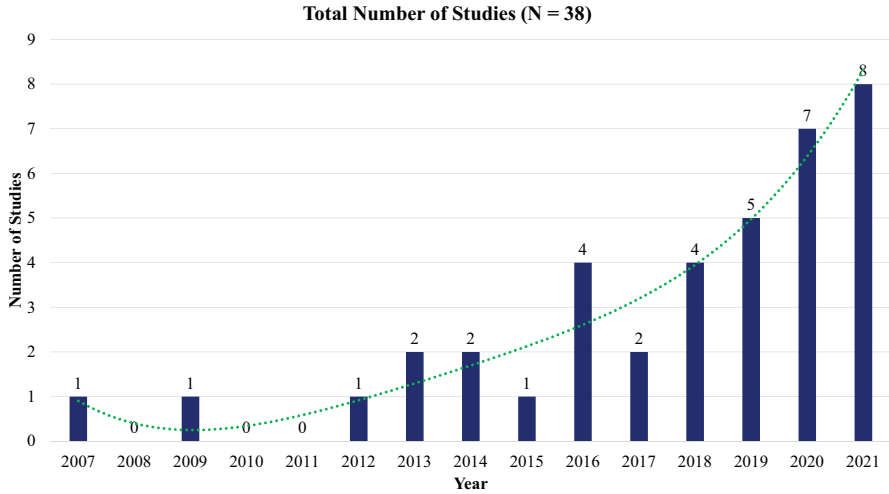
Fig. 1 Research methodology flowchart

reviewed articles’ titles, abstracts, and keywords. The analysis revealed emerging themes based on the extant literature. In this study, the major themes that emerged were around resources, risks, and implications and, last but not least, strategies employed to mitigate or overcome resource shortages in supply chains. Second, a critical taxonomy of the reviewed articles was performed to identify the causes of major resource shortages and corresponding mitigation strategies.

### 3 Results

#### 3.1 Literature Landscape

The search results revealed that the area of resource shortages and scarcity in supply chains did not emerge in scholarly journals until 2016 and had been established since then. The number of publications has been steadily growing. Indeed, from 2007 to 2015, the number of publications per year was quite limited. However, in 2016 a peak in the number of relevant published articles was observed, demonstrating the increasing interest in resource shortages and scarcity issues in supply chains, hence



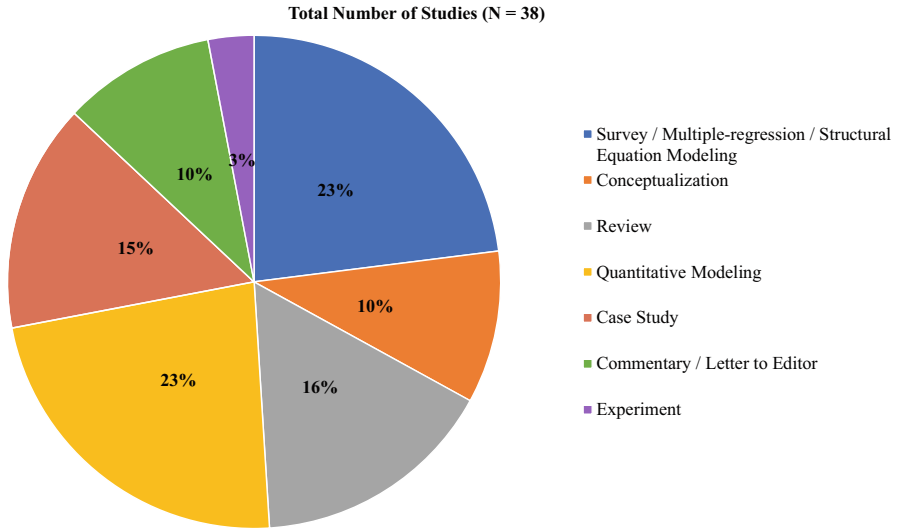
**Fig. 2** Distribution of publications by year

establishing it as a new research area. The main reason for this growing interest in the domain can be attributed to the even more emerging need to make supply chains more resilient due to the COVID-19 pandemic and other developments such as the Brexit Referendum. Figure 2 depicts the annual allocation of the reviewed publications over the last years.

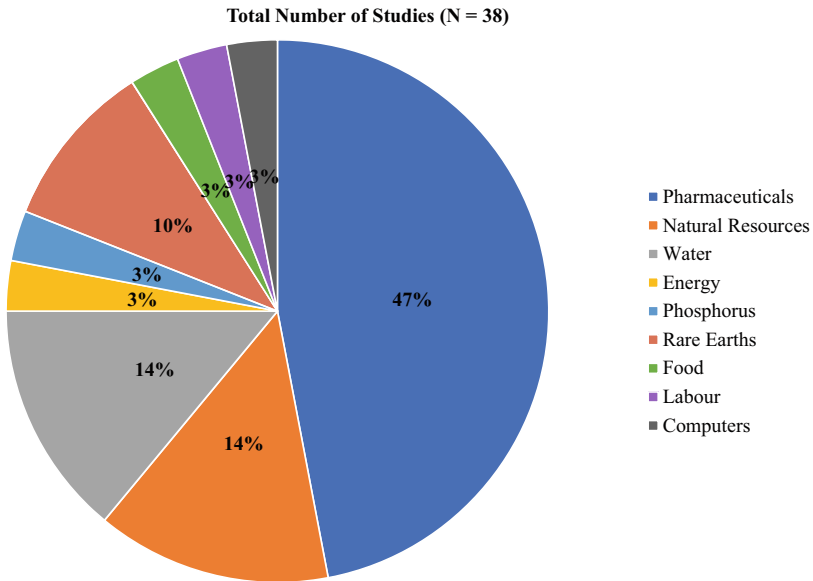
Concerning the methodology approach, seven categories emerged (see Fig. 3). The descriptive statistical analysis results show that 23% of the studies use quantitative modeling approaches, with life cycle analysis being used to assess the utilization of specific resources. Furthermore, 23% of the reviewed studies applied survey and multiple regression analysis or structural equation modeling to test hypothesized relationships. Moreover, 16% of the reviewed studies used secondary data to conduct literature reviews. The 15% employed case studies to thoroughly examine the field and provide the researcher(s) with primary evidence [68]. A few papers were conceptual in nature and tried to develop theory and propositions (10%) or were letters to the editor and commentaries (10%). Experimental research was conducted in only one study. Although there is a myriad of empirical works attempting to explore and understand shortages and scarcity impacts on different industries, most analyses have not been guided by a formal theoretical framework. Only six papers employed a theory in their research, including the resource advantage theory, the resource dependency theory, the theory of constraints, the capability maturity theory, and the resilience theory.

Most of the reviewed papers investigated the pharmaceutical sector and drug shortages (47%), whereas 14% of the studies focused on multiple natural resources, whereas 14% focused only on water scarcity issues. Shortages of rare earth metals were also a concern in 10% of the studies, and a few studies focused on other resources such as labor and food (see Fig. 4).



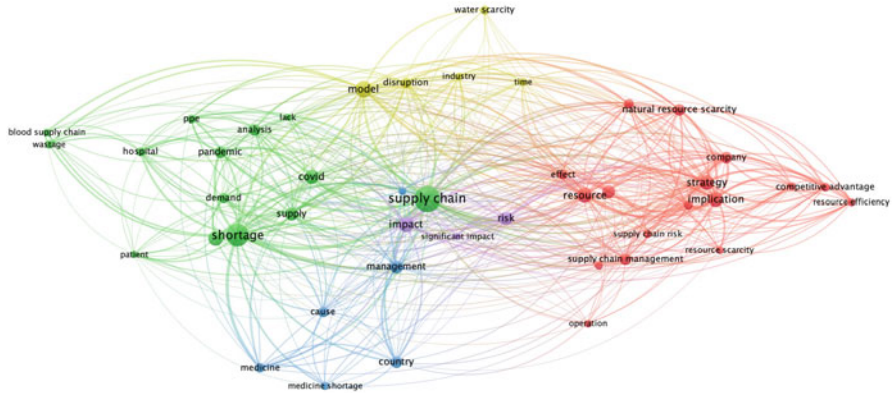


**Fig. 3** Employed research methodology



**Fig. 4** Documented resources experiencing shortages

A bibliometric analysis of the selected articles’ title, abstract, and keywords highlighted emerging themes (Fig. 5). In particular, the bibliometric map indicates five thematic categories (highlighted as clusters of terms in a different color). Central to these thematic areas are the “supply chain,” “shortage,” “impact,” “resource,” and



**Fig. 5** Bibliometric map and terms’ co-occurrence of the selected articles (generated by VOSviewer 1.6.18 software)

“management.” The connections’ thickness denotes the strength of the link between terms; the minimum number of terms’ co-occurrence was set to five.

### 3.2 Causes of Resource Shortages

Disruptions and “black swan” events challenge the resilience of supply chains in diverse economy segments, reveal vulnerabilities, and ultimately lead to product shortages that impact downstream operations in both public and private sectors. The major causes of resource shortages, as identified via the critical taxonomy of the reviewed literature, are henceforth discussed. Table 1 inserts a critical taxonomy of significant causes of resource shortages in supply chains.

**Supply Disruptions** The most apparent cause of goods shortages is raw material unavailability and supply instability upstream of a supply chain. Global population growth, emerging markets, and elevated consumption patterns are inherently associated with a high rate of natural resource appropriation to satisfy the required human needs and demands [5]. The “non-renewable” character of some resource types (e.g., coal, oil, and minerals) further contributes to supply shortages, while overexploitation creates ecosystem imbalances [12].

The observed volatility in materials’ supply can also be attributed to political disturbances that may disrupt the supply flow of materials, specifically in markets where raw material sources are concentrated. Political instability is particularly relevant to the case of rare minerals. For example, Zaire is the leading supplier of cobalt; however, in 1978, insurgents from Angola occupied the Shaba Province and blocked the power supply to the regional mining facilities, thus resulting in flooding and evacuation on the part of contractors for about 5 days [5]. In addition,

**Table 1** Main causes of resource shortages in supply chains – a critical taxonomy

Main category	Causes	References
Supply disruptions	Limited raw material availability	Acosta et al. [1], Aljaded et al. [3], Alonso et al. [5], Cogan et al. [15], Rajendran and Ravi Ravindran [50], Yatskovskaya et al. [67]
	Overexploitation of resource bases to meet human needs	Alonso et al. [5], Bell et al. [12], El Wali et al. [22], Koh et al. [37], Reich-Weiser and Dornfeld [51], Yatskovskaya et al. [67]
	Geopolitical developments	Grose and Richardson [26], Kalaitzi et al. [34], Lapko et al. [39], Wiedmer et al. [66]
	Climate change and natural/manmade disasters	Awad et al. [8], de Vries et al. [19], Grose and Richardson [26], Porkka et al. [47], Reich-Weiser and Dornfeld [51], Sharma et al. [53], Socal et al. [55], Sutcliffe et al. [57], Wiedmer et al. [66]
	Price fluctuations	Acosta et al. [1], de Paulo Farias and dos Santos Gomes [18], Kalaitzi et al. [34]
Demand instability	Emerging markets & consumers' panic buys (demand intensity)	Bell et al. [13], Cohen and Rodgers [16], de Vries et al. [19], Grose and Richardson [26], Mehrotra et al. [45], Porkka et al. [47], Slowinski et al. [54], Socal et al. [55], Voas and Ksherti [63], Wiedmer et al. [66]
	Policy-making amendments	Iyengar et al. [29], Krautkraemer [38]
Manufacturing constraints	Manufacturing inflexibility and lack of interchangeability	Acosta et al. [1], Lozano-Diez et al. [42], Sodhi et al. [56]
	Complex manufacturing processes and quality considerations	Awad et al. [8], Cogan et al. [15], de Vries et al. [19], Jia and Zhao [32], Tucker et al. [60], Zwaida et al. [71]
Policy inconsistencies	Inadequate management of stockpiles	Sodhi et al. [56]
	Lengthy regulatory procedures	Awad et al. [8]
Economic considerations	Low prices of resources	Cogan et al. [15], Large et al. [40], Socal et al. [55]
	High supply chain and market concentration	Alonso et al. [4], Cogan et al. [15], El Wali et al. [22], Jia and Zhao [32], Kalaitzi et al. [34], Slowinski et al. [54]

geopolitical developments could interrupt the regular supply of essential supplies. For example, in 2011, China reduced export quotas of rare earth oxides, leading to shortages of components in automotive catalysts [39].

Moreover, supply instability due to natural/manmade disasters (e.g., earthquakes and pandemics), except for disruptions in operations, leads to price volatility. The food crisis in 2007–2008 resulted in significant price increases for several commodities with subsequent implications for global food security [18].

**Demand Instability** Resource scarcity designates the imbalance of physical supply and demand [38]. Therefore, instability at the dipole supply demand in supply chains leads to goods shortages, particularly in rapidly occurring fluctuations. The resulting shortages occur due to supply chains' struggles to increase and orchestrate supply and production operations to the levels necessary to satisfy backlogs and respond to demand spikes. For example, at the start of the COVID-19 pandemic, the backlog to restock personal protective equipment (PPE) in some countries ranged between 6 and 12 months [23]. In addition, supply uncertainty and consumers' cautions often trigger the bullwhip effect as retailers tend to increase order quantities, particularly during prolonged periods of disruption [58].

Furthermore, changes in policy-making levels often trigger demand surges that, in tandem with production inflexibility and responsiveness, ultimately lead to market shortages. For example, the inclusion of the meningitis B vaccine in the UK childhood immunization program in 2015 caused a rapid increase in demand, leading to supply shortages [29].

**Manufacturing Constraints** To date, most manufacturing systems operate according to batch processing, meaning that large volumes of goods are manufactured per production cycle without being able to adapt manufacturing parameters and accommodate diverse product specifications. Furthermore, the lack of production interchangeability further highlights this inflexibility. A documented case is that of commercial and household paper products during the COVID-19 pandemic, where manufacturing systems' inflexibility led to prolonged shortages of household paper products, e.g., toilet paper, paper towels, and disinfectant wipes [56].

Furthermore, manufacturing complexities associate with quality vulnerabilities that often result in production halts. The latter case is evident in pharmaceuticals, where violation of good manufacturing practices necessitates additional inspections and approval from the FDA to resume production operations [32]. Such facility shutdowns for a considerable amount of time lead to medicine shortages.

**Policy Inconsistencies** Stockpiles of critical supplies require robust management processes to ensure appropriate inventory levels and resource usability in emergencies. For example, the National Strategic Stockpile of PPE and medical supplies in the USA were critical to promptly responding to the COVID-19 pandemic. However, demand surges over 100 times above the extant National Stockpile, and the distribution to the states of expired essential equipment suggests inadequate management of the National Stockpile by the US Department of Health and Human Services [56].

Furthermore, regulatory and legislative processes significantly relate to resource shortages. Indicatively, complex and lengthy drug approval procedures can either demotivate manufacturers from entering/remaining in a market or lead to unexpected delivery delays, thus contributing to shortages (e.g., drug shortages in Jordan in 2004) [8].

**Economic Considerations** Low prices of resources, specifically human capital, can impact occupational and organizational commitment, as in the documented case of truck drivers in Europe [40]. To a greater extent, the pricing of resources could trigger market reconfigurations that lead to resource shortages. Low prices and low-profit margins in non-patented pharmaceuticals result in high market concentration that limits the possibility of identifying alternative sourcing options, potentially leading to drug shortages under market pressure [32].

### 3.3 *Mitigation Strategies*

Proactive resilience planning should be initiated to mitigate the risks of resource shortages. Mitigation strategies are designed and adopted to achieve resilience based on the type of risk, the position of the company within the supply chain, and the disruption impacts on the company and the supply chain [9, 21, 41]. Resilience development efforts and the implementation of such strategies to prevent resource shortages should occur at the company level (e.g., product and process redesign) and/or supply chain level (e.g., supply chain reconfiguration). The mitigation strategies that are most widely documented highlight the need for policy development, control and monitoring of supply and demand, technology advancement, inventory management, product and process redesign, development of supply chain relationships, resource recovery strategies, and logistics reconfiguration. Table 2 inserts a critical taxonomy of mitigation strategies for resource shortages in supply chains stemming from the reviewed studies.

**Policy Development** Around the globe, the number of shortages regarding different resources is rising. For example, since the outbreak of the COVID-19 pandemic, there have been shortages of materials in the construction industry, and it is expected to worsen due to the Russia–Ukraine war as energy prices will continue to soar. Thus, there is a need for specific policies and regulatory interventions to help ease pressures and mitigate the shortage disruptions.

In the pharmaceutical industry, studies document a need to develop a national digital platform that will enable the search for resources and products by multiple suppliers to establish a warning system for shortages [8]. Most specifically, this system will act as a formal communication channel to monitor policies and transactions to enable reporting and notification of current or expected shortages [3]. In such a digital platform, policy should articulate specific steps and guidelines for managing shortages, such as (i) identifying information about substitute drugs to devise a prioritization list of alternative therapies during shortages and (ii) retrieving

**Table 2** Mitigation strategies for resource shortages in supply chains – a critical taxonomy

Mitigation strategy	Specific practices	Benefits	References	Resources or industry
Policy development	<p>Establish a national reporting system for shortages</p> <p>Strengthen the local capacity to maintain and distribute stockpiles by establishing medicines exchange programs</p> <p>Consider an industrial policy to incentivize production and increase domestic production</p> <p>Introduce stock and lead time requirements</p> <p>Address trade and tax policies to keep global trade open</p> <p>Incentivize more companies to enter and stay in markets encountering shortages</p>	<p>Formal communication channel and advanced notifications about expected future shortages</p> <p>Reduced dependence ensuring sufficient, uninterrupted supply</p>	<p>Acosta et al. [1]; Aljazeera et al. [3]; Alonso et al. [4, 5]; Awad et al. [8]; Bastani et al. [11]; Cogan et al. [15]; Cohen and Rodgers [16]; de Paulo Farias and dos Santos Gomes [18]; de Vries et al. [19]; Iyengar et al. [29]; Socal et al. [55]; Tucker et al. [60]</p>	<p>Drugs/pharmaceuticals; PPE</p>
Control and monitoring of supply and demand	<p>Proactively analyze foreign markets</p> <p>Improve supply chain agility</p> <p>Communicate information about plans and stock data earlier and in more detail to more partners</p> <p>Map essential supply chain resources</p> <p>Investigate suppliers' and manufacturers' locations regarding resource availability and life cycle assessment</p> <p>Improve customer culture and knowledge</p>	<p>Enhanced ability to anticipate product shortages</p> <p>Developing a culture of rational resource use</p>	<p>Awad et al. [8]; Bastani et al. [11]; Cogan et al. [15]; Koh et al. [37]</p>	<p>Drugs/pharmaceuticals</p>
Technology advancement	<p>Automate inventory management system – employ special software and centralized databases</p> <p>Automate product dispensing systems</p> <p>Adopt Industry 4.0 technologies</p> <p>Adopt technologies to explore new (alternative) resources and use more sustainable substitute materials</p> <p>Develop a public digital platform to monitor multiple suppliers</p>	<p>Real-time management of inventory</p> <p>Minimized waste and shortages</p> <p>Efficient material planning and enhanced transparency and visibility</p>	<p>Aljazeera et al. [3]; Alonso et al. [4, 5]; Awad et al. [8]; Bastani et al. [11]; Iyengar et al. [29]; Lapko et al. [39]; Mehrotra et al. [45]; Sutcliffe et al. [57]</p>	<p>Drugs/pharmaceuticals; water</p>

(Continued)

Table 2 (Continued)

Mitigation strategy	Specific practices	Benefits	References	Resources or industry
Inventory management	Increase inventory levels of critical resources Develop proper inventory models	Improved resource availability	Alonso et al. [4]; Awad et al. [8]; Mehrotra et al. [45]; Rajendran and Ravi Ravindran [50]; Sutcliffe et al. [57]; Tucker et al. [60]	Drugs/pharmaceuticals; water
Product and process redesign	Substitute materials by using alternative resources or suppliers Adopt initiatives for sustainability Improve production efficiency Avoid using scarce natural resources (if possible) Use occupational safety and health hazard precautionary measures for workers and product safety	Improved management of shortages	Aljadede et al. [3]; Alonso et al. [4, 5]; Awad et al. [8]; Bell et al. [13]; de Vries et al. [19]; Iyengar et al. [29]; Kalaitzi et al. [35]; Koh et al. [37]; Lapko et al. [39]; Sharma et al. [53]; Tucker et al. [60]; Yatskovskaya et al. [67]	Drugs/pharmaceuticals; labor; natural resources
Supply chain relationships development	Increase cooperation between the public and the private sectors Establish long-term agreements and partnerships Introduce contractual amendments such as strengthening failure-to-supply clauses	Improved resource availability	Awad et al. [8]; Kalaitzi et al. [34, 35]; Koh et al. [37]; Lapko et al. [39]; Maghsoudi et al. [43]; Sutcliffe et al. [57]; Tucker et al. [60]; Yatskovskaya et al. [67]	Drugs/pharmaceuticals; humanitarian aid; water
Resource recovery	Adopt recycling practices Develop closed-loop capabilities Adopt remanufacturing practices	Ongoing manufacturing of products by recovered resources	Alonso et al. [4, 5]; Bell et al. [12, 13]; El Wali et al. [22]; Kalaitzi et al. [34, 35]; Lapko et al. [39]	Natural resources (e.g., water, metals, and phosphorus)
Logistics reconfiguration	Design multi-modal and multi-route contingency plans Operationalize logistics techniques, where resources are shifted to sites suffering from local scarcity Develop logistics strategies to reduce food losses and waste	Enhanced flexibility of transportation – shortened lead times	Alonso et al. [4, 5]; Bell et al. [12]; de Paulo Farias and dos Santos Gomes [18]	Natural resources

suppliers' information in case of shortages to enable the redistribution of medicines across warehouses or healthcare facilities [1, 3, 8, 29]. The data needed to be captured from pharmaceuticals' manufacturing capacities are around eligible drugs, pricing, procurement sources (e.g., eligible domestic suppliers), availability, quality, and technical specifications of medicines [29, 55]. For a successful healthcare system, there is a need to improve the cooperation between the private and public sectors to enhance resource availability and ensure sufficiency and uninterrupted supply [8, 15].

Another practice is rationalizing the distribution of resources to cope with scarcity or shortages and the ban or limitation in the quantities of exports to protect national supplies. During the COVID-19 pandemic, a company in Europe ordered protective masks and disinfection gel from a supplier in Singapore, but the order never arrived. The same happened when the German government ordered masks from Kenya, but the shipment never arrived. Moreover, supermarkets limited the quantities of products consumers could purchase to manage stock levels. Awad et al. [8] suggested a need for public education campaigns (e.g., conducting seminars and developing supporting brochures) to help consumers, patients, and healthcare service providers rationalize drug use and educate them regarding medication alternatives.

Local sourcing is another mitigation strategy that emerges in times of resource shortages to increase supply chain resilience. Past studies referred to the reshoring of production operations [5]. Aljadeed et al. [3] focused on medicines and PPE availability in Saudi Arabia and highlighted the need to support local manufacturers in producing such essential products. de Vries et al. [19] also suggested the practice of reshoring the production of critical supplies in Europe; hence, there is a need to offer financial incentives to motivate manufacturers to produce medicines in Europe. Cohen and Rodgers [16] also referred to the need to incentivize and increase the US production of PPE and medical supplies to minimize the dependence on the global supply chain. Thus, reshoring success depends on more substantial incentives and authorizations for pharmaceutical companies to enter and stay in the market [15, 29, 55]. Moreover, cross-country medicines exchange programs [3] and a mutual agreement between the US and European regulators could be established to recognize available manufacturing facilities and process inspections [55].

In the food industry, the reshoring practice was also mentioned by de Paulo Farias and dos Santos Gomes [18], who identified the necessity of supporting smallholder farmers to enhance their productivity and introducing trade and tax policies to secure global trade operations. Regarding regulatory changes, Acosta et al. [1], Aljadeed et al. [3], de Vries et al. [19], and Tucker et al. [60] mentioned additional practices to remove shortage disruptions such as pooling demand from multiple countries, introducing legislative actions by requiring companies to maintain redundancy, adopting penalty policy to prevent price gouging, limiting or restricting parallel exports, and signing longer-term contracts with manufacturers.

**Control and Monitoring of Supply and Demand** To get greater visibility over their supply network regarding the origin and availability of resources, companies



should map their supply network by capturing information from all suppliers. Thus, supply chain mapping will enable identifying and managing the resources' interconnectedness to their point of origin so inefficient resource practices can be recognized [37]. This practice can also be considered an initiative to enhance information sharing during disruptions that lead to shortages [19]. For example, Reich-Weisser and Dornfeld [51] focused on water scarcity and argued that both supplier and manufacturing locations must be known along with the resource availability to inform location planning and selection that can impact water availability. Many companies encounter growing water scarcity worldwide, e.g., India and the USA, and reconfigure their supply networks to respond to the increasing pressures to limit consumption.

Apart from the importance of location, focal companies and their suppliers should also develop strategies to enhance stakeholders' awareness of their capacities [8]. First, companies need to quantify the resource requirements at each manufacturing stage for comparison and control; for some resources, such as water, a regional rather than global life cycle approach should be considered [51]. Focused analyses (e.g., hotspot and life cycle assessment) can reveal water-intensive manufacturing processes to inform alternative water mitigation policies and practices, e.g., resource recovery or product and process redesign [2, 7].

Companies also need to control and monitor the inertia or "resistance to change" regarding resource utilization and management [37]. Monitoring and control will enable companies to establish a notification system for public stakeholders (e.g., about water resources appropriation) or national medicines regulatory authorities (e.g., about pharmaceutical inventory) [29]. Moreover, Awad et al. [8] discussed that manufacturing companies in the pharmaceutical industry should increase their share of the national market and improve the local demand forecasting for their products. In this effort, there is a need to improve customer culture and knowledge by (i) rationalizing the prescription of medications and informing customers about medication consumption [11] and (ii) sharing adequate information (e.g., through media) to assure customers that companies can deal with specific issues/incidents and there is an efficient national and local safety stock and adequate supply (e.g., toilet paper).

**Technology Advancement** Shortage issues can be overcome by the support of technology to develop substitutes or exploit alternative natural resources [5]. Furthermore, there is a need to automate inventory management by applying advanced models and special software [8]. There is also a need to enhance information technology capabilities to achieve strategic partnerships. Digital applications can enable efficient material planning by leveraging real-time information flows to enhance the transparency and visibility of the supply chain. Kalaitzi et al. [35] also mentioned the challenge for many companies to achieve transparency for specific materials. The challenge derives from the reluctance among suppliers to share information; thus, companies need to prioritize the visibility of scarce materials for critical component suppliers.

Sharma et al. [53] highlighted the need to invest in Industry 4.0 technologies (such as the Internet of things, big data analytics, and digital twins) to enable transparency and visibility. Overall, Industry 4.0 technologies promise to manufacture goods with better efficiency and reduced resource consumption [31]. Regarding water pressure and irrigation in agriculture, Sutcliffe et al. [57] found that growers did not apply efficient technologies such as drip irrigation or center pivots but continued to implement hose reels fitted with rain guns and booms.

**Inventory Management** Sutcliffe et al. [57] suggested buffering water resources to mitigate shortages, leading to financial loss. Kalaitzi et al. [35] also referred to safety stock as a practice for resources such as water, but it cannot easily be applied for metals and rare earth elements due to price volatility and because it ties up cash unnecessarily. This practice has also been discussed regarding pharmaceuticals or healthcare provision services (e.g., in hospitals) and is essential to be applied by all stakeholders across a supply chain [8]. Therefore, the purpose of safety stock is to hold enough inventory to account for unanticipated shortages. Cogan et al. [15] further stated that companies in the pharmaceutical industry must change and employ more agile inventory management practices for antibiotics and improve transparency through better communication with partners about their operations planning.

de Vries et al. [19] referred to the European Union Directive 2001/83, where certain Member States place obligations on pharmacies and impose penalties if the desired inventory is not available. For example, Norway implemented a “prepositioning duty” for wholesalers, and the Netherlands considered obliging wholesalers and manufacturers to maintain a strategic stock covering 5 months of demand for all medicines [19]. In this sense, shortages could be reduced by holding safety stock ([27]; [30]); however, holding this inventory is a relatively expensive policy option. To this effect, monitoring and optimizing the stock of resources are essential [60].

**Product and Process Redesign** Product design enables the suppliers to know product manufacturing resource requirements based on suppliers’ capabilities and the shortages of resources [5]. The involvement of suppliers in product design can minimize the risk of material shortages [44]. The global chip shortages led many companies to redesign their products, so fewer chips are needed. In addition, Koh et al. [37] pointed out the need to invest in sustainability initiatives by applying process redesign or supply chain reengineering by first identifying specific resource constraints. Another practice is substitution, i.e., using alternative materials that are more abundant [5, 35, 39]. Acosta et al. [1], Bastani et al. [11], and Iyengar et al. [29] also mentioned the exploration of alternative yet approved substitute medicines.

Moreover, another documented practice was extending expiry dates and changing the quality requirements for batches of safe but substandard medicines. de Vries et al. [19] mentioned this practice; however, there is a need to set rules or guidelines on substituting medicines that are out of stock in the pharmaceutical industry. Last but not least, during the COVID-19 pandemic, many shortages emerged due to nationwide lockdowns and safety measures. Therefore, companies had to redesign

their internal systems using precautionary health hazard measures (e.g., facemasks and gloves) and technical solutions (e.g., robots and cobots) for worker support and product safety purposes [48].

**Supply Chain Relationship Development** Kalaitzi et al. [35] referred to three primary supply chain relationships, i.e., transactional, relational, and hierarchical, which can be used to minimize or overcome shortage issues. Companies shall establish transactional, long-term contracts for commodity resources (even when few suppliers exist), e.g., fixed-term contracts for water, gas, and electric power. Contractual changes such as strengthening failure-to-supply clauses and increasing prices are also mentioned in the extant literature [60].

Companies use relational mechanisms, i.e., partnerships and joint ventures, to achieve discretion over resources. For example, GlobalFoundries and the Ford Motor Company developed a strategic collaboration, so more chips are delivered to Ford in the short term with a promising long-term collaboration in the automotive industry. de Vries et al. [19] also emphasized the need to develop strong supplier relationships to ensure continuity of access to resources. Sutcliffe et al. [57] mentioned collaboration as the primary management response to mitigate the risk of water shortages. The authors outlined the need for collaboration to prepare the appropriate infrastructure to allow water transfers across regions for fulfilling cultivation needs.

Additionally, through mergers and acquisitions, vertical supply chain integration can be applied to acquire or control essential resources. Limited suitable suppliers or government regulations that restrict the accessibility to specific resources make vertical integration a preferred strategy. For instance, Housebuilder Persimmon and Tesla avoided the disruption of supply chain shortages with vertical integration.

Another mitigation practice is the use of multi-sourcing to diversify the supply chain. Due to tariff wars, uncertainty in supply chains can be mitigated by not relying on single-sourcing options for critical supplies. This strategy will help to avoid any monopoly formations [19] and ensure a “*supply base that can be drawn upon in the event of a failure*” ([52], p. 98). Thus, maintaining several suppliers is an effective way to minimize the risk of shortages.

**Resource Recovery** Many studies referred to the circular economy and material recovery methods such as recycling to increase the availability of scarce resources [13]. For example, Kalaitzi et al. [34] found that manufacturing companies recycle resources such as water and metals to respond to the implications of natural resource scarcity. Other studies also referred to the recycling of resources such as platinum or cobalt (e.g., [4]). Kalaitzi et al. [34] mentioned that companies use recycled materials such as aluminum as these resources do not decrease in quality, whereas water and plastic suffer from quality loss and cannot be recycled infinitely. Bell et al. [13] highlighted the competitive advantage that a company could gain through closed-loop recycling, i.e., recycling and reusing post-consumer goods to extract and supply material for manufacturing the same products.

Recently, scholars and policymakers started to explore the possibility of transitioning from linear to circular economy business models [37]. According to

Velenturf et al. [62], the circular economy entails various practices such as design for durability, reuse and reparability, recycling, and recovering materials. For example, the growing demand for electric vehicles and the competition between original equipment manufacturers for scarce resources show the significance of recycling end-of-life batteries. Thus, the circular economy requires action across multiple stakeholders such as government, industry, NGOs, and academia. In addition, the design of products for circularity should follow certain specifications for them to be easily repairable. Indicatively, IKEA sells used, secondhand furniture that has been refurbished; the company also initiated a buy-back scheme for customers to return unwanted furniture and other items. El Wali et al. [22] studied the recapturing and recycling of phosphorus to use it more efficiently. Although this practice is one of the most widely adopted, companies cannot recycle all resources due to high cost or technical aspects and the need to develop recycling infrastructure [5]. Moreover, resources such as plastic are exported to other countries, mainly to Asia, where the recycling standards are less stringent than in Europe.

**Logistics Reconfiguration** Every company depends on logistics operations, i.e., quick and cost-effective shipments and storage of raw materials and products. However, the logistics industry encounters diverse challenges, e.g., shortages of drivers and limited transport/warehouse capacity due to various factors such as the COVID-19 pandemic, Brexit, and armed conflicts. Consequently, logistics interventions are emphasized in the literature as a response to resource shortages [19] due to the potential to improve transport and storage flexibility (e.g., having multi-modal and multi-route contingency plans for disruptions). Another logistics-centric technique suggested by Bell et al. [13] stresses the option to transfer resources to sites suffering from local scarcity. The same approach was also mentioned by de Paulo Farias and dos Santos Gomes [18], who stressed that companies in the food industry have to focus on critical logistics bottlenecks to ensure the viability of operations in the food value chain. Notably, the authors referred to the implementation of logistics strategies to minimize shortages and waste, deriving from restrictions in transport routes and social distance measures.

## 4 Conclusions

Supply chains in most industries encounter resource shortages. Several factors, especially with long-lasting disruptive effects such as pandemics and climate change, challenge operations managers and decision-makers regarding the management of limited resources. For example, the most recent disruption that substantially impacted global supply chains is the COVID-19 pandemic, which negatively affected customer service level, production scheduling and planning, lead time, and financial performance. Several authors highlighted the implications of the pandemic on supply chains in various sectors (e.g., demand uncertainty from consumers and trading partners, labor shortages, and product deficiencies), which led to increased

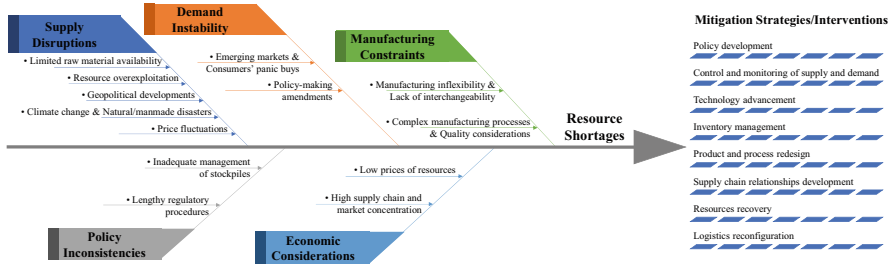


Fig. 6 Drivers of resource shortages and respective mitigation strategies framework

gaps between supply and demand [25, 28]. Numerous strategies were applied to mitigate the emanating disruptions, such as utilizing additive manufacturing, holding increased safety stock, revising production plans, and fostering collaborations [49].

In this research, a critical literature taxonomy was conducted to explore the causes of resource shortages and identify mitigation strategies in a supply chain context. Our analysis revealed various documented factors leading to resource shortages, e.g., limitations in the production output, natural disasters, social forces (e.g., strikes), inaccurate forecasting, unexpected demand surges of specific resources, and limited availability of alternative suppliers [36]. Except for disruptions in manufacturing logistics operations, shortages can have severe economic and social impacts; e.g., a shortage of antibiotics may cost up to US\$20–30 million and further lead to an increased mortality rate [10].

In particular, the literature search and thematic analysis revealed five main categories of root causes for resource shortages, namely (i) supply disruptions; (ii) demand instability; (iii) manufacturing constraints; (iv) policy inconsistencies; and (v) economic considerations (see Fig. 6). Identifying the causes of shortages is the first step in a lengthy and complex process of change, and our research indicates that a comprehensive effort is needed to overcome shortages crises. Additionally, eight categories of strategies emerged to manage shortages, specifically (i) policy development; (ii) control and monitoring of supply and demand; (iii) technology advancement; (iv) inventory management; (v) product and process redesign; (vi) supply chain relationships development; (vii) resources recovery; and (viii) logistics reconfiguration.

In the short term, actors operating at various supply chain echelons can increase inventory levels of critical resources (at the expense of holding cost, though), develop proper inventory management models, and adopt sustainability initiatives to overcome shortages. Furthermore, medium- and long-term investments and incentives will be required to improve resource availability. For example, governments need to develop policies to motivate and increase domestic production capacity. Therefore, policymakers must incentivize more companies to enter and stay in markets encountering shortages.

Moreover, firms need to explore and apply appropriate methods such as life cycle assessment and value chain mapping of essential supply chain resources and communicate data and information about available resource stocks to achieve more transparency across supply chains and identify potential risks of shortages. In the face of shortages and scarcity, previous studies discussed innovative management practices, e.g., substitution and avoidance of usage of scarce resources, recycling, implementation of circular economy principles, and remanufacturing. These mitigation strategies require policy changes, investments, and supply chain reconfigurations. Additionally, collaboration among various public and private stakeholders is needed. Buyers and suppliers need to establish long-term agreements and partnerships. Finally, resource shortages that emerged during the COVID-19 pandemic highlighted the need for reshoring and raised new doubts about offshoring and/or outsourcing production to distant countries.

In the future, several factors will persist and continue leading to shortages (e.g., lockdowns stemming from China's zero-COVID-19 strategy have stretched domestic and international supply chains and have significantly increased operational risks for companies). Others just emerged (e.g., the Russia-Ukraine war that led to disruptions in the European supply of natural gas, crude oil, and agricultural commodities – the German Interior Minister advised citizens to keep an inventory of food and essentials for 10 days in connection with the war in Ukraine and the possible power outages) or will emerge (e.g., supply chain cyber-attacks). To build supply chain resilience, organizations need to adopt a more proactive attitude instead of the traditional reactive approach to disruptions.

## References

1. Acosta, A., Vanegas, E.P., Rovira, J., Godman, B., Bochenek, T.: Medicine shortages: gaps between countries and global perspectives. *Front. Pharmacol.* **10**, 763 (2019)
2. Aivazidou, E., Tsolakis, N., Vlachos, D., Iakovou, E.: A water footprint management framework for supply chains under green market behaviour. *J. Clean. Prod.* **197**, 592–606 (2018)
3. Aljadeed, R., Alruthia, Y., Balkhi, B., Sales, O., Alwhaibi, M., Almohammed, O., Alotaibi, A.J., Alrumaih, A.M., Asiri, Y.: The impact of covid-19 on essential medicines and personal protective equipment availability and prices in Saudi Arabia. *Healthcare.* **9**(3), 290 (2021)
4. Alonso, E., Field, F.R., Roth, R., Kirchain, R.E.: Strategies to Address Risks of Platinum Scarcity for Supply Chain Downstream Firms, pp. 1–6. IEEE International Symposium on Sustainable Systems and Technology, Washington, DC (2009)
5. Alonso, E., Gregory, J., Field, F., Kirchain, R.: Material availability and the supply chain: risks, effects, and responses. *Environ. Sci. Technol.* **41**(19), 6649–6656 (2007)
6. Althaf, S., Babbitt, C.W.: Disruption risks to material supply chains in the electronics sector. *Resour. Conserv. Recycl.* **167**, 105248 (2021)
7. Anastasiadis, F., Tsolakis, N.: Environmental hotspots analysis: A systematic framework for food supply chains and implementation case in the UK poultry industry. *J. Clean. Prod.* **305**, 126981 (2021)
8. Awad, H., Al-Zu'bi, Z., Abdallah, A.: A quantitative analysis of the causes of drug shortages in Jordan: A supply chain perspective. *Int. Bus. Res.* **9**(6), 53–63 (2016)

9. Baghersad, M., Zobel, C.W.: Assessing the extended impacts of supply chain disruptions on firms: an empirical study. *Int. J. Prod. Econ.* **231**, 107862 (2021)
10. Baraldi, E.: Causes of Antibiotic Shortages and the Solutions to Address Them. Global Antibiotic Research & Development Partnership. <https://revive.gardp.org/causes-of-antibiotic-shortages-and-the-solutions-to-address-them/>. Last accessed 2022/04/09 (2021)
11. Bastani, P., Sadeghkhani, O., Ravangard, R., Rezaei, R., Bikine, P., Mehralian, G.: Designing a resilience model for pharmaceutical supply chain during crises: A grounded theory approach. *J. Pharm. Policy Pract.* **14**, 115 (2021)
12. Bell, J.E., Autry, C.W., Mollenkopf, D.A., Thornton, L.M.: A natural resource scarcity typology: theoretical foundations and strategic implications for supply chain management. *J. Bus. Logist.* **33**(2), 158–166 (2012)
13. Bell, J.E., Mollenkopf, D.A., Stolze, H.J.: Natural resource scarcity and the closed-loop supply chain: A resource-advantage view. *Int. J. Phys. Distrib. Logist. Manag.* **43**, 351–379 (2013)
14. Christopher, M., Peck, H.: Building the resilient supply chain. *Int. J. Logist. Manag.* **15**, 1–14 (2004)
15. Cogan, D., Karrar, K., Iyer, J.K. Shortage, stockouts and scarcity: The issues facing the security of antibiotic supply and the role for pharmaceutical companies. [https://www.amrbenchmark.org/media/uploads/downloads/5d848ddd0b2ac\\_Antibiotic-Shortages-Stockouts-and-Scarcity\\_Access-to-Medicine-Foundation\\_31-May-2018.pdf](https://www.amrbenchmark.org/media/uploads/downloads/5d848ddd0b2ac_Antibiotic-Shortages-Stockouts-and-Scarcity_Access-to-Medicine-Foundation_31-May-2018.pdf). Last accessed 2022/03/09 (2018)
16. Cohen, J., Rodgers, Y.V.D.M.: Contributing factors to personal protective equipment shortages during the COVID-19 pandemic. *Prev. Med.* **141**, 106263 (2020)
17. Cohen, M.A., Kouvelis, P.: Revisit of AAA excellence of global value chains: robustness, resilience, and realignment. *Prod. Oper. Manag.* **30**(3), 633–643 (2021)
18. de Paulo Farias, D., dos Santos Gomes, M.G.: COVID-19 outbreak: what should be done to avoid food shortages? *Trends Food Sci. Technol.* **102**, 291–292 (2020)
19. de Vries, H., Jahre, M., Selviaridis, K., van Oorschot, K., van Wassenhove, L.: A Review of Scientific and Grey Literature on Medicine Shortages and the Need for a Research Agenda in Operations and Supply Chain Management. BI Norwegian Business School, Oslo (2021)
20. Denyer, D., Tranfield, D.: Producing a systematic review. In: Buchanan, D., Bryman, A. (eds.) *The Sage Handbook of Organizational Research Methods*, pp. 671–689. Sage, London (2009)
21. Dolgui, A., Ivanov, D., Rozhkov, M.: Does the ripple effect influence the bullwhip effect? An integrated analysis of structural and operational dynamics in the supply chain. *Int. J. Prod. Res.* **58**(5), 1285–1301 (2020)
22. El Wali, M., Golroudbary, S.R., Kraslawski, A.: Circular economy for phosphorus supply chain and its impact on social sustainable development goals. *Sci. Total Environ.* **777**, 146060 (2021)
23. Frost & Sullivan: The COVID-19 Pandemic's Impact on the Global Healthcare Personal Protective Equipment Market. Frost & Sullivan (2020)
24. Garousi, V., Felderer, M., Mäntylä, M.V.: Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Inf. Softw. Technol.* **106**, 101–121 (2019)
25. Govindan, K., Mina, H., Alavi, B.: A decision support system for demand management in healthcare supply chains considering the epidemic outbreaks: A case study of coronavirus disease 2019 (COVID-19). *Trans. Res. Part E Logist. Transp. Rev.* **138**, 101967 (2020)
26. Grose, J., Richardson, J.: Strategies to identify future shortages due to interruptions in the health care procurement supply chain and their impact on health services: A method from the English National Health Service. *J. Health Serv. Res. Policy.* **19**(1), 19–26 (2014)
27. Gupta, D.K., Huang, S.-M.: Drug shortages in the United States: A critical evaluation of root causes and the need for action. *Clin. Pharmacol. Ther.* **93**(2), 133–135 (2013)
28. Ivanov, D.: Predicting the impacts of epidemic outbreaks on global supply chains: A simulation-based analysis on the coronavirus (COVID-19/SARS-CoV-2) case. *Transp. Res. Part E Logist. Transp. Rev.* **136**, 101922 (2020)
29. Iyengar, S., Hedman, L., Forte, G., Hill, S.: Medicine shortages: A commentary on causes and mitigation strategies. *BMC Med.* **14**(1), 124 (2016)



30. Jarosławski, S., Azaiez, C., Korchagina, D., Toumi, M.: Quantifying the persisting orphan-drug shortage public health crisis in the United States. *J. Market Access Health Policy*. **5**(1), 1269473 (2017)
31. Javaid, M., Haleem, A., Singh, R.P., Suman, R., Gonzalez, E.S.: Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. *Sustain. Oper. Comput.* **3**, 203–217 (2022)
32. Jia, J., Zhao, H.: Mitigating the U.S. drug shortages through Pareto-improving contracts. *Prod. Oper. Manag.* **26**(8), 1463–1480 (2017)
33. Jüttner, U., Maklan, S.: Supply chain resilience in the global financial crisis: an empirical study. *Supply Chain Manag. Int. J.* **16**, 246–259 (2011)
34. Kalaitzi, D., Matopoulos, A., Bourlakis, M., Tate, W.: Supply chain strategies in an era of natural resource scarcity. *Int. J. Oper. Prod. Manag.* **38**(3), 784–809 (2018)
35. Kalaitzi, D., Matopoulos, A., Bourlakis, M., Tate, W.: Supply chains under resource pressure: strategies for improving resource efficiency and competitive advantage. *Int. J. Oper. Prod. Manag.* **39**(12), 1323–1354 (2019)
36. Kalaitzi, D., Matopoulos, A., Fornasiero, R., Sardesai, S., Barros, A.C., Balech, S., Muerza, V.: Megatrends and trends shaping supply chain innovation. In: Fornasiero, R., Sardesai, S., Barros, A.C., Matopoulos, A. (eds.) *Next Generation Supply Chains*, pp. 3–34. Springer, Cham (2021)
37. Koh, S.C.L., Gunasekaran, A., Morris, J., Obayi, R., Ebrahimi, S.M.: Conceptualizing a circular framework of supply chain resource sustainability. *Int. J. Oper. Prod. Manag.* **37**(10), 1520–1540 (2017)
38. Krautkraemer, J.A.: *Economics of Natural Resource Scarcity: the State of the Debate Discussion Paper 05–14*. Resources for the Future, Washington DC (2005)
39. Lapko, Y., Trucco, P., Nuur, C.: The business perspective on materials criticality: evidence from manufacturers. *Resour. Policy*. **50**, 93–107 (2016)
40. Large, R.O., Breitling, T., Kramer, N.: Driver shortage and fluctuation: occupational and organizational commitment of truck drivers. *Supply Chain Forum Int. J.* **15**(3), 66–72 (2014)
41. Li, Y., Chen, K., Collignon, S., Ivanov, D.: Ripple effect in the supply chain network: forward and backward disruption propagation, network health and firm vulnerability. *Eur. J. Oper. Res.* **291**(3), 1117–1131 (2021)
42. Lozano-Diez, J.A., Marmolejo-Saucedo, J.A., Rodriguez-Aguilar, R.: Designing a resilient supply chain: an approach to reduce drug shortages in epidemic outbreaks. *EAI Endorsed Trans. Pervasive Health Technol.* **6**(21), e2 (2020)
43. Maghsoudi, A., Zailani, S., Ramayah, T., Pazirandeh, A.: Coordination of efforts in disaster relief supply chains: the moderating role of resource scarcity and redundancy. *Int J Log Res Appl.* **21**(4), 407–430 (2018)
44. McCormack, K., Wilkerson, T., Marrow, D., Davey, M., Shah, M., Yee, D.: *Managing Risk in your Organization with the SCOR Methodology*. The Supply Chain Council Risk Research Team. <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.668.3730&rep=rep1&type=pdf>. Last accessed 2022/03/09 (2008)
45. Mehrotra, P., Malani, P., Yadav, P.: Personal protective equipment shortages during COVID-19 – supply chain-related causes and mitigation strategies. *JAMA Health Forum.* **1**(5), e200553 (2020)
46. Nagurney, A.: Supply chain game theory network modeling under labor constraints: applications to the Covid-19 pandemic. *Eur. J. Oper. Res.* **293**(3), 880–891 (2021)
47. Porkka, M., Gerten, D., Schaphoff, S., Siebert, S., Kumm, M.: Causes and trends of water scarcity in food production. *Environ. Res. Lett.* **11**(1), 015001 (2016)
48. Ragasa, C., Lambrecht, I.: COVID-19 and the food system: setback or opportunity for gender equality? *Food Secur.* **12**, 877–880 (2020)
49. Raj, A., Mukherjee, A.A., de Sousa Jabbour, A.B.L., Srivastava, S.K.: Supply chain management during and post-COVID-19 pandemic: Mitigation strategies and practical lessons learned. *J. Bus. Res.* **142**, 1125–1139 (2022)



50. Rajendran, S., Ravi Ravindran, A.: Inventory management of platelets along blood supply chain to minimize wastage and shortage. *Comput. Ind. Eng.* **130**, 714–730 (2019)
51. Reich-Weiser, Dornfeld, D.A.: A discussion of greenhouse gas emission tradeoffs and water scarcity within the supply chain. *J. Manuf. Syst.* **28**(1), 23–27 (2009)
52. Sénat République Française. Pénuries de médicaments et de vaccins: Renforcer l'éthique de santé publiques dans la chaîne du médicament. <https://www.senat.fr/notice-rapport/2017/r17-737-notice.html>. Last accessed 2021/04/10 (2018)
53. Sharma, R., Shishodia, A., Kamble, S., Gunasekaran, A., Belhadi, A.: Agriculture supply chain risks and COVID-19: mitigation strategies and implications for the practitioners. *Int. J. Log. Res. Appl.* (2020). <https://doi.org/10.1080/13675567.2020.1830049>
54. Slowinski, G., Latimer, D., Mehlman, S.: Dealing with shortages of critical materials. *Res. Technol. Manag.* **56**(5), 18–24 (2013)
55. Socal, M.P., Sharfstein, J.M., Greene, J.A.: The pandemic and the supply chain: gaps in pharmaceutical production and distribution. *Am. J. Public Health.* **111**(4), 635–639 (2021)
56. Sodhi, M.S., Tang, C.S., Willenson, E.T.: Research opportunities in preparing supply chains of essential goods for future pandemics. *Int. J. Prod. Res.* **61**(1), 1–16 (2021)
57. Sutcliffe, C., Know, J., Hess, T.: Managing irrigation under pressure: how supply chain demands and environmental objectives drive imbalance in agricultural resilience to water shortages. *Agric. Water Manag.* **243**, 106484 (2021)
58. Terlep, S., Gasparro, A.: Why Are There Still Not Enough Paper Towels? *Wall Street Journal*, <https://www.wsj.com/articles/why-arent-there-enough-paper-towels-11598020793>. Last accessed 2022/03/12 (2020)
59. Tranfield, D., Denyer, D., Smart, P.: Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *Br. J. Manag.* **14**(3), 207–222 (2003)
60. Tucker, E.L., Daskin, M.S., Sweet, B.V., Hopp, W.J.: Incentivizing resilient supply chain design to prevent drug shortages: policy analysis using two- and multi-stage stochastic programs. *IIE Trans.* **52**(4), 394–412 (2020)
61. van Hoek, R.: Research opportunities for a more resilient post-COVID-19 supply chain – closing the gap between research findings and industry practice. *Int. J. Oper. Prod. Manag.* **40**(4), 341–355 (2020)
62. Velenturf, A.P.M., Purnell, P., Macaskie, L., Sapsford, D., Mayes, W.: Chapter 1: A new perspective on a global circular economy. In: Macaskie, L., Sapsford, D., Mayes, W. (eds.) *Resource Recovery from Wastes: Towards a Circular Economy*, pp. 1–22. Royal Society of Chemistry, London (2019)
63. Voas, J., Ksherti, N.: Scarcity. *IEEE Comput.* **54**(1), 26–28 (2021)
64. Watson, R.T., Webster, J.: Analysing the past to prepare for the future: writing a literature review a roadmap for release 2.0. *J. Decis. Syst.* **29**(3), 129–147 (2020)
65. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: writing a literature review. *MIS Q.* **26**(2), xiii–xxiii (2002)
66. Wiedmer, R., Whipple, J.M., Griffis, S.E., Voorhees, C.M.: Resource scarcity perceptions in supply chains: the effect of buyer altruism on the propensity for collaboration. *J. Supply Chain Manag.* **56**(4), 45–64 (2020)
67. Yatskovskaya, E., Srari, J.S., Kumar, M.: Integrated supply network maturity model: water scarcity perspective. *Sustainability.* **10**(3), 896 (2018)
68. Yin, R.K.: *Case Study Research: Design and Methods*, 3rd edn. SAGE Publications, Thousand Oaks (2003)
69. Young, D., Hutchinson, R., Reeves, M.: The Green Economy Has a Resource-Scarcity Problem. <https://hbr.org/2021/07/the-green-economy-has-a-resource-scarcity-problem>. Last accessed 2022/02/24 (2021)
70. Zhong, L., Wu, B., Morrison, A.M.: Research on China's tourism: A 35-year review and authorship analysis. *Int. J. Tour. Res.* **17**(1), 25–34 (2015)
71. Zwaيدا, T.A., Beauregard, Y., Elarroudi, K.: Comprehensive literature review about drug shortages in the Canadian hospital's pharmacy supply chain. In: 2019 International Conference on Engineering, Science, and Industrial Applications (ICESI), pp. 1–5. Institute of Electrical and Electronics Engineers Inc., Tokyo (2019)

# Critical Infrastructure Detection During an Evacuation with Alternative Fuel Vehicles



Chrysaifis Vogiatzis and Eleftheria Kontou

## 1 Introduction

In this chapter, we investigate the problem of evacuating residents within an urban network setting where we have vehicles of different fuel types. While conventional fossil-fueled vehicles have typically access to a well-established network of refueling stations, vehicles of newer and alternative fuel technologies still face limitations on the number of refueling stations and, consequently, have difficulties accessing refueling infrastructure reliably. Hence, during an evacuation procedure, an adversary may decide to pose a *hybrid threat*. While the immediate natural or anthropogenic threat (e.g., hurricane, nuclear plant accident, flooding, etc.) is taking place, an adversary may opt to “attack” the plan in order to cause the evacuation to fail. The adversarial attack can be physical (as in, attacking existing infrastructure) or virtual (in the form of a cyberattack or a misinformation campaign). Hence, it becomes important for evacuation planners and managers to know in advance the roads that are fundamental to the success of the plan so as to fortify them and consider alternatives in case of failure during the evacuation. The novelty in our approach lies with the fact that we consider different vehicles with different refueling needs when making the decisions for fortifying part of the evacuation plan.

---

C. Vogiatzis (✉)

Industrial and Enterprise Systems Engineering, University of Illinois at Urbana-Champaign, Urbana, IL, USA

e-mail: [chrys@illinois.edu](mailto:chrys@illinois.edu)

E. Kontou

Civil and Environmental Engineering, University of Illinois at Urbana-Champaign, Urbana, IL, USA

e-mail: [kontou@illinois.edu](mailto:kontou@illinois.edu)

This chapter is organized as follows. In the remainder of Sect. 1, we offer a brief literature review. We then proceed to present the basic framework we work with, along with the mathematical programming formulation in Sect. 2. Section 3 provides a new betweenness variant that we then use to solve our problem heuristically. We present an indicative case study in Sect. 4 by applying the problem to a well-known transportation network benchmark instance, the Sioux Falls transportation network. We then conclude this work and offer insight into interesting future work in Sect. 5.

## ***1.1 Alternative Fuel Vehicles***

While market penetration of alternative fuel vehicles is constantly growing [1], access to reliable infrastructure networks for energy supply and resilience of operations remain major challenges (e.g., [2, 3]). During evacuations, drivers of emerging vehicle technologies, like electric ones, can be stranded due to limited driving range and transportation network's disruptions. Policymakers in the United States, EU, and other regions around the world set ambitious goals of alternative fuel vehicles adoption; for instance, in the United States, decision-makers target 50% electric vehicle sales by 2030 [4]. Mass transitions to alternative fuel cars will reduce vehicles' range (e.g., from 403 miles of median range for a conventional vehicle to 234 miles of median range for an electric one [5]) and increase dependencies to a sparse energy supply infrastructure network. Hazardous events and emergencies, exacerbated by climate change [6], will only magnify issues faced by alternative fuel vehicle drivers [7, 8]. Emergency coordinators and managers play an important role in creating preemptive evacuation plans for vulnerable alternative fuel vehicle users and safeguarding them from adverse conditions. In the existing literature, such plans typically address single threats (e.g., [9, 10]) and are fast, convergent (i.e., tree graph), one-directional (i.e., contraflow), and enable reliable access to refueling infrastructure [11]. Current evacuation path designs do not focus on fortification strategies, even though hybrid threats in this context can have catastrophic consequences, such as loss of property and life. Thus, addressing hybrid threats in evacuation planning by identifying critical infrastructure in evacuation networks of alternative fuel vehicles is both a scientific and practical challenge that this chapter aims to address.

## ***1.2 Evacuation and Disaster Management***

Evacuation is a traffic assignment problem, with drivers found to prefer familiar routes and interstates [12] while simulation is often used to solve such dynamic problems [13]. Evacuation routing and path designation literature has treated this problem as a network flow one that minimizes total travel time using exact or

heuristic algorithms to get solutions (e.g., [14–16]). Designated evacuation routes often have desirable characteristics like seamlessness for ease of route signage and avoidance of evacuees’ confusion [17, 18], contraflow that enables the reversal of links on the network for increased road capacity and faster evacuations [19], and practical access to refueling networks by evacuees via rerouting them through respite sites [11, 20]. Due to the advent of alternative fuel vehicles, research is addressing access to energy supply networks for, for example, electric vehicles, by estimating delays at charging stations [10], and designing routes for reaching safety [9, 11].

### 1.3 Threats to Evacuation and Transportation

Transportation networks are one of the most fundamental systems that we rely on every single day. According to *Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience*, transportation systems (including road transportation) is one of the critical infrastructure sectors [21]. In the same document, some of the threat/attack vectors that are outlined against transportation networks are natural disasters (e.g., hurricanes), cyberattacks, and terrorist attacks on the highway system. With the increased reliance on cyber systems to control automated vehicles and traffic control, cyberattacks could cause highways to close down especially during the most inopportune time (as in when a large-scale evacuation is under way). Additionally, the existence of legacy control systems in transportation only exacerbates the threat [22]. Hence, the identification of critical infrastructure before an evacuation takes place is of utmost importance as it will allow for both fortifying the infrastructure and providing us with time to think of alternatives.

### 1.4 Critical Element Detection

Detecting critical elements (i.e., nodes, edges, or other structures) in networks has been especially prominent over the last 20 years. With the interest of research in network analysis growing toward network vulnerability and survivability, more and more studies have focused on the detection of elements whose failure or disruption causes significant changes. This is evidenced by the increasing number of surveys in the topic (see, e.g., [23, 24]). In traditional critical node detection problems, the setup is as follows. Given a graph  $G(V, E)$  and a connectivity metric  $\mathcal{C}(G)$ , does there exist a set of nodes  $S \subset V$  of cardinality  $|S| \leq k$  such that  $\mathcal{C}(G[V \setminus S]) \leq \ell$ ? In the previous definition, we use  $G[S]$  to denote the subgraph of  $G(V, E)$  that is induced by  $S \subseteq V$ . A similar setup can be posed for detecting critical edges.

As the definition of the connectivity metric  $\mathcal{C}(G)$  changes, we obtain different variants. However, so long as the property that the new graph  $G[V \setminus S]$  needs to satisfy upon removal of  $S$  is nontrivial and hereditary, then the critical node

detection problem is  $\mathcal{NP}$ -hard [25]. This is why we often resort to other views of criticality or “importance” to solve these types of problems.

Such another view of criticality or “importance” comes from centrality and its relationship to network vulnerability [26]. Later in this work, we propose a variant of a traditionally used centrality metric to identify roads of importance in our evacuation plans. That said, centrality is a vast field of research with applications in areas as diverse as computational biology [27–29], student networks [30, 31], the social sciences (see, e.g., [32]), criminal network analysis [33], and, of course, transportation [34–36].

A brief history of centrality should always begin in the late 1940s and the fundamental contributions of Bavelas [37, 38], which assigned importance to nodes. Later, contributions by Anthonisse [39] and Freeman [40, 41] would spur new betweenness-based importance metrics: these metrics relied on the assumption that the exchange of information between two actors would traverse through their shortest path in the network, making the intermediate nodes and edges critical. More recently, extensions have been proposed to capture new ideas in network analysis. These ideas range from residual centrality [42] (where the importance of a node is quantified by its impact upon removal or deactivation) to group centrality [43–45] and the centrality of induced clusters (such as cliques [46, 47], stars [48, 49], and others [50]). Centrality measures (and specifically betweenness) have been applied in evacuation (see, e.g., [51, 52]); however, in our case, we employ them in a slightly different manner.

Specifically, in this work, we use a variant of betweenness centrality to identify crucial roads to our evacuation plans. The metric and its details are presented in Sect. 3.

## 2 Framework

In this section, we provide the necessary notation and fundamentals, the problem definition, and, finally, the full mathematical formulation.

### 2.1 Notation and Fundamentals

Let  $G(V, E)$  be a directed graph that represents the transportation network. There exists some node  $s \in V$  that is treated as the shelter: that is, a safe location that vehicles in our transportation network aim to reach during the evacuation process. Moreover, we assume the existence of a set of different types of vehicles  $K$ . Every vehicle  $k \in K$  requires different refueling infrastructure. For example,  $K = \{\text{gas, electric, hydrogen}\}$  would imply the existence of three types of vehicles: traditional gas-operated vehicles, electric vehicles, and vehicles with hydrogen cells.

Each node  $i \in V$  is associated with a demand  $q_i^k$ , which is different for each vehicle type  $k \in K$ . Moreover, certain nodes may serve as refueling centers for vehicle type  $k \in K$ : if that is the case, we define  $\alpha_i^k = 1$ , otherwise  $\alpha_i^k = 0$ . We also assume that each vehicle of type  $k \in K$  begins with a “full tank.” We define that quantity as  $R^k$ . For simplicity, and in order to avoid dealing with queuing at refueling stations, we assume that every vehicle spends the same amount of time to refuel. This time, denoted as  $\tau^k$ , is only dependent on the type of vehicle. As an example, conventional gas vehicles could require less time to fully refuel than electric vehicles.

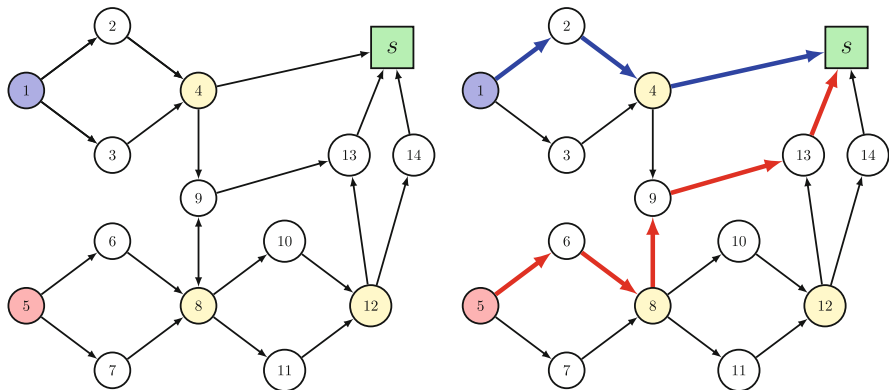
Finally, every edge  $(i, j) \in E$  is associated with two parameters:  $t_{ij}$  and  $\phi_{ij}^k$ . The former is the time it takes to traverse the edge. The latter is the amount of fuel that traversing the edge requires. Note how the amount of fuel is different for each vehicle type  $k$ , implying that some vehicles may need to spend more fuel than others. If each edge only required  $\phi_{ij}^k = 1$ , then this could be viewed as a “hop”-constrained version of the problem, similar to the one studied in [11].

## 2.2 Problem Definition

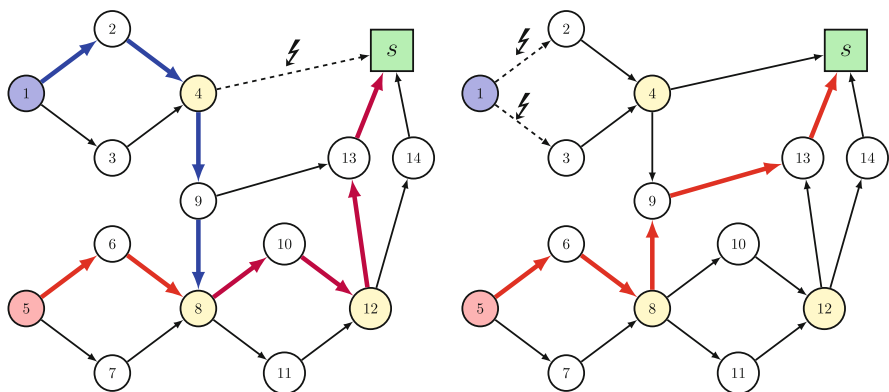
We are now ready to provide the formal problem definition. We consider the case of an evacuation planner or disaster manager that is deciding on the routes that different types of vehicles will need to follow during an evacuation. At the same time, we also consider the existence of an adversary that aims to disrupt these plans by disrupting a set of edges in the network. We assume that when an edge is disrupted, vehicles are unable to use it. Of course, if the adversary disrupts all edges leading to refueling stations, then vehicles that are located far from the shelter would be unable to reach their destination.

From the evacuation planning side, we consider the evacuation tree problem [17, 18]. In an evacuation tree, vehicles are forced to follow one path to safety. This implies that at no point in the evacuation route are vehicles allowed to bifurcate and follow two or more different paths. This renders the evacuation process more seamless and easier to follow and coordinate. Since in our case we are dealing with a set of vehicle types  $K$ , we will also be identifying  $|K|$  evacuation trees. To ensure the success of the evacuation routing, evacuation trees for different vehicles are not allowed to conflict. This implies that if the evacuation tree for conventional gas vehicles uses a specific street, the evacuation tree for a different vehicle fuel type is only allowed to use that same street in the same direction, or not at all.

Additionally, vehicles are required to refuel in order to reach their final destination safely. To achieve that, our evacuation trees will need to be built in a way that vehicles have access to their unique refueling infrastructure when they need to. Once the evacuation routes are built, the adversary will select a set of edges to disrupt of cardinality at most equal to their budget,  $B$ . Our problem then poses the question: “Which are the edges/streets that are most important for the well-being



**Fig. 1** In this indicative example, there are 100 vehicles of fuel type 1 with  $R = 2$  waiting to evacuate from node 1; as well as 50 vehicles of fuel type 2 with  $R = 3$  waiting to evacuate from node 5. The shelter is located in the northwest corner. Nodes 4, 8, and 12 are refueling stations for both types of vehicles. The network is presented in (a). The evacuation trees for the two demand nodes are shown in (b)



(a) The resultant evacuation trees after the adversary attacks 1 edge.

(b) The resultant evacuation trees after the adversary attacks 2 edges.

**Fig. 2** Here we show the optimal adversary attacks with a budget of one or two edges. For one edge, the optimal course of action for the adversary is shown in (a), along with the new evacuation tree. The solution for a budget of two edges is presented in (b)

of our evacuation process?” We depict the problem with the following indicative example. Assume that we are evacuating two locations (nodes 1 and 2) using the transportation network shown in Fig. 1.

In Fig. 2, we note that given a budget that is big enough, the adversary will try to completely close down the path of as many vehicles as possible (see, e.g., Fig. 2b, where the 100 vehicles at node 1 have no way of escaping). On the other hand, with

limited budget, the adversary will try to upend the evacuation process of as many vehicles as possible.

For example, in Fig. 2a, we see that even though the adversary only blocks one road, this causes quite the change in the evacuation plan. For starters, vehicles of type 1 starting from node 1 have to completely change their route; they cannot simply get re-routed to node 9 and 13 before reaching safety, because they do not have the fuel to do so. Instead, they need to refuel at node 8 (and again at node 12) prior to reaching safety. At the same time, the evacuation plan for vehicles at node 5 also needs to change as they can no longer use the road connecting node 8 to node 9. Using it would cause a conflict between vehicles that have originated from node 1 and are headed to refueling.

Finally, we observe that the optimal solutions for the adversary are not hereditary: that is, the set of optimal edges to disrupt for budget  $B_1$  is not necessarily a subset of the set of optimal edges to disrupt for budget  $B_2$  when  $B_1 < B_2$ . Assume we had an increased budget of three edges in our indicative toy example, then we would prefer to disrupt the edge from  $B = 1$  (the one connecting node 4 to safety) and completely disconnect node 5; furthermore, if we had a budget of four edges, then we would opt to disconnect both nodes 1 and 5, leading to stranding all vehicles before they can evacuate.

### 2.3 Mathematical Formulation

After the notation and the problem definition, we are finally ready to present our mathematical formulation. We begin with the evacuation planning problem, that is, the inner problem.

Let  $f_{ij}$  be the flow on arc  $(i, j) \in E$ . Now, the flow on that arc can have originated from many different nodes. We then define  $f_{ijm}^k$  as the flow on arc  $(i, j) \in E$  that originated from  $m \in V$  and is for vehicles of fuel type  $k$ . Note how this variable is only defined over the set of nodes  $m \in V$  and fuel types  $k \in K$  such that  $q_m^k > 0$ . We also define  $x_{ij}^k$  as a binary variable that indicates whether an edge is part of the evacuation tree for vehicles of fuel type  $k$ . If  $x_{ij}^k = 0$ , this immediately implies that vehicles of fuel type  $k$  are not allowed to use edge  $(i, j)$ .

We also define two decision variables to keep track of fuel and refueling operations. Variables  $r_{im}^k$  keep track of the fuel that vehicles of type  $k$  that originated from node  $m$  have when reaching node  $i \in V$ . Note that we assume that all vehicles start with full fuel, and hence  $r_{mm}^k = R^k$ . We also allow vehicles to refuel when needed so that they may reach the shelter. If a vehicle is set to refuel at node  $i$  (provided node  $i$  has the proper refueling infrastructure for vehicle type  $k$ ), then we set binary variable  $w_{im}^k = 1$ .

With these variable definitions at hand, and alongside the notation introduced earlier in Sect. 2.1, we are now ready to present the full formulation in (2).



Specifically, in the objective function of (2a) we minimize the total time to have every vehicle evacuate. The time consists of both the travel time (assumed to be linear) and the time to refuel at a refueling station along the way. Constraints (2b) define variables  $f_{ij}$  by consolidating all flow from every origin and of every vehicle fuel type. Constraints (2c) force the existence of evacuation trees; specifically, they enforce that there can be at most one outgoing arc used from every node in the network. Constraints (2d) stop conflicts among the evacuation trees by prohibiting them from going in the opposite directions. Continuing, in constraints (2e), we only allow flow of a specific type of vehicle on an arc if it is part of the corresponding evacuation tree. For now, we assume a big- $M$  capacity over here; however, that could be replaced with actual capacities when those are available. Constraints (2f) and (2g)–(2i) keep track of the fuel of each vehicle. The former “starts” every vehicle on a “full tank”; the latter two state that a vehicle will either spend  $\phi_{ij}^k$  amount of fuel to traverse an arc or will fully refuel. To control where vehicles are allowed to refuel, we have constraints (2j). Continuing, (2k) are the traditional flow preservation constraints. Finally, (2l)–(2p) provide the variable restrictions, as those were defined earlier in the section.

Note how this problem, solved by the evacuation planners, is referred to as *Evac*. Now, let us bring the adversary to the mix. Given a budget  $B$ , the adversary will select a set of edges of cardinality at most  $B$  with the sole goal of disrupting our evacuation plans. Let  $y_{ij} = 1$  if and only if the adversary disrupts edge  $(i, j)$ . We then define the set of all feasible solutions for the adversary (i.e., all combinations of edges they can remove within their budgetary constraint) as

$$\mathcal{Y} = \left\{ y \in \{0, 1\}^{|E|} : \sum_{(i,j) \in E} y_{ij} \leq B \right\}.$$

Moreover, let

$$\mathcal{X}(y) = \left\{ (x, f, f_m^k, w, r) : (2b)–(2p) \text{ are satisfied and } x_{ij}^k \leq 1 - y_{ij}, \forall (i, j) \in E \right\}.$$

Then, the bilevel optimization problem can be formulated as in (1).

$$\max_{y \in \mathcal{Y}} \min_{(x, f, f_m^k, w, r) \in \mathcal{X}(y)} z \quad (1)$$

In the next section, we propose a heuristic based on a variant of betweenness to tackle this problem.

$$\begin{aligned}
 (Evac) : \min z = & \sum_{(i,j) \in E} t_{ij} f_{ij} + \sum_{i \in V, m \in V, k \in K: q_m^k > 0} q_m^k \tau^k w_{im}^k & (2a) \\
 & \sum_{m \in V, k \in K: q_m^k > 0} f_{ijm}^k = f_{ij}, & (2b) \\
 & \forall (i, j) \in E, \\
 & \sum_{j: (i,j) \in E} x_{ij}^k \leq 1, & (2c) \\
 & \forall i \in V, \forall k \in K, \\
 & x_{ij}^k + x_{ji}^\ell \leq 1, & (2d) \\
 & \forall (i, j) \in E, \forall k, \ell \in K, \\
 & f_{ijm}^k \leq M \cdot x_{ij}^k, & (2e) \\
 & \forall (i, j) \in E, \forall m \in V, k \in K : q_m^k > 0, \\
 & r_{mm}^k = R^k, & (2f) \\
 & \forall m \in V, k \in K : q_m^k > 0, & (2g)
 \end{aligned}$$

$$r_{jm}^k \leq \left( r_{im}^k - \phi_{ij}^k x_{ij}^k + M \cdot \left( 1 - x_{ij}^k \right) \right) \cdot \left( 1 - w_{jm}^k \right) + R^k w_{jm}^k, \quad (2h)$$

$$r_{jm}^k \geq \left( r_{im}^k - \phi_{ij}^k x_{ij}^k - M \cdot \left( 1 - x_{ij}^k \right) \right) \cdot \left( 1 - w_{jm}^k \right) + R^k w_{jm}^k, \quad (2i)$$

$$w_{im}^k \leq \alpha_i^k, \quad \forall i \in V, \forall m \in V, k \in K : q_m^k > 0, \quad (2j)$$

$$\sum_{j:(i,j) \in E} f_{ijm}^k - \sum_{j:(j,i) \in E} f_{ijm}^k = \begin{cases} q_m^k, & \text{if } i = m \\ -q_m^k, & \text{if } i = s \\ 0, & \text{otherwise.} \end{cases} \quad (2k)$$

$$x_{ij}^k \in \{0, 1\}, \quad \forall (i, j) \in E, \forall k \in K, \quad (2l)$$

$$f_{ijm}^k \geq 0, \quad \forall (i, j) \in E, \forall m \in V, k \in K : q_m^k > 0, \quad (2m)$$

$$f_{ij} \geq 0, \quad \forall (i, j) \in E, \quad (2n)$$

$$w_{im}^k \in \{0, 1\}, \quad \forall i \in V, \forall m \in V, k \in K : q_m^k > 0, \quad (2o)$$

$$r_{im}^k \geq 0, \quad \forall i \in V, \forall m \in V, k \in K : q_m^k > 0. \quad (2p)$$

### 3 Side-Constrained Betweenness Heuristic

Before providing the heuristic algorithm, we begin this section with the intuition behind the proposed side-constrained betweenness centrality metric.

#### 3.1 Intuition

Consider a vehicle of fuel type  $k$  evacuating from some node  $i$  toward the designated shelter. For simplicity, let us assume that the fuel required for traversing every edge is normalized to be equal to 1 (this is also referred to as “hop”-constrained, see [11]). Moreover, let  $d_{ij}$  be the shortest path distance (i.e., geodesic distance) connecting nodes  $i$  to  $j$ . In our case, we are interested in the shortest path to the shelter, and hence, we define  $d_{is}, \forall i \in V$ .

If  $d_{is} > R^k$ , then vehicles of fuel type  $k$  originating from node  $i$  will need to refuel prior to reaching the designated safety zone. This refueling process could potentially happen multiple times. For example, if a vehicle is located at node  $i$  such that  $d_{is} \leq R^k$ , then it can reach safety with the fuel it currently has; if  $\ell \cdot R^k < d_{is} \leq (\ell + 1) \cdot R^k$ , then it will require at least  $\ell$  refueling stops.

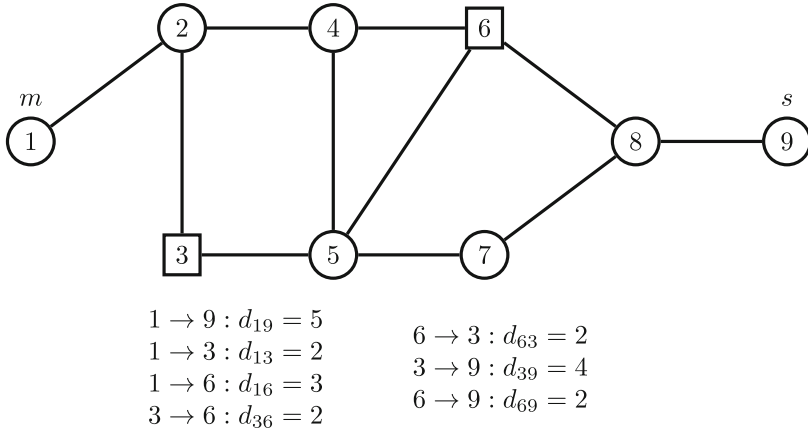
Granted, in the original evacuation tree problem, no vehicle is guaranteed to use its shortest path to safety in order to ensure a safe, seamless, and robust evacuation plan. However, we can use this intuition as a heuristic approach in order to identify important streets that we need to protect. We now present the algorithm in the next subsections.

#### 3.2 Side-Constrained Betweenness Centrality

In traditional *shortest path* betweenness centrality [40, 41, 53, 54], we are concerned with the fraction of shortest paths between any two nodes  $i, j$  that pass through node  $h$ . In our case, we deal with the edge-based variant [39] where we are concerned with the fraction of shortest paths between any two nodes  $i, j$  that use edge  $e$ . Specifically, let  $\sigma_{ij}$  be the total number of shortest paths connecting nodes  $i, j$ , and let  $\sigma_{ij}(e)$  be the number of shortest paths connecting node  $i, j$  that use edge  $e \in E$ . Then

$$b_e = \sum_{i \in V} \sum_{j \in V} \frac{\sigma_{ij}(e)}{\sigma_{ij}}.$$

In this variant, betweenness centrality with refueling considerations, we are interested in the most important edges when reaching a terminal node  $s$  starting from any node such that we respect the fuel constraints. Vehicles of type  $k$  originating



**Fig. 3** In this simple graph, nodes 3 and 6 are the only available refueling stations. We then calculate seven shortest paths: from the origin  $m$  to the terminal node/shelter  $s$ , from  $m$  to each of the refueling stations, between all refueling stations, and from the refueling stations to  $s$

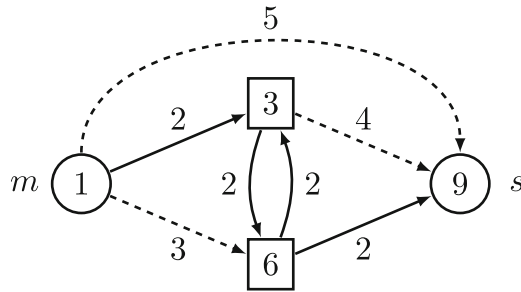
from node  $m \in V$  will need to refuel at any of the nodes  $i \in V$  such that  $\alpha_i^k = 1$ . To solve the problem, we follow a three-step approach for each origin  $m \in V$  and each fuel type  $k$ .

**Step 1: All Shortest Paths Calculation**

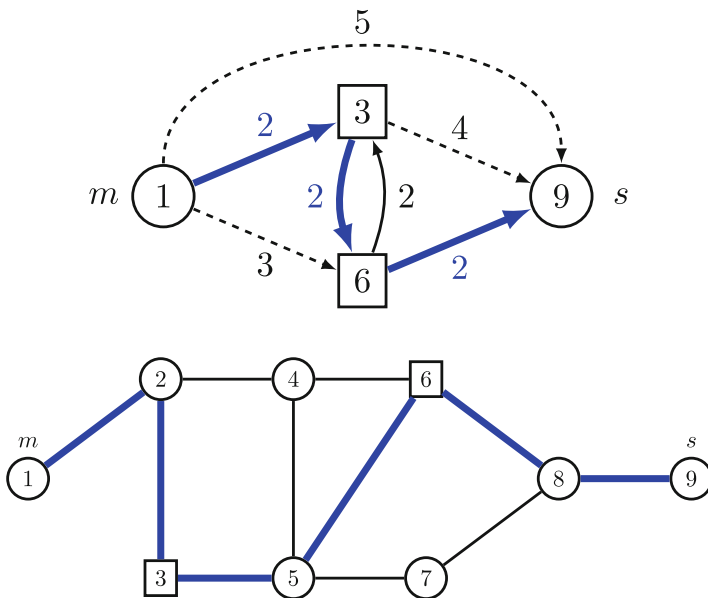
We begin by calculating all shortest paths between any origin node  $m \in V$  and all refueling stations and the shelter node. We also calculate all shortest paths between any two refueling stations of type  $k$  (i.e., between any two nodes  $i, j$  such that  $\alpha_i^k = \alpha_j^k = 1$ ). Finally, we calculate all shortest paths between any refueling station of type  $k$  and the shelter node. We visualize these calculations in Fig. 3.

**Step 2: Building Refueling Graph**

With all shortest paths from the first step, we build a new graph that only includes the specific origin node, the shelter, and all refueling station nodes. In this new graph  $G_m^k$ , we only connect two nodes if the shortest path between them is smaller than or equal to  $R^k$ . We show the construction in Fig. 4 for a vehicle of fuel type  $k$  with  $R^k = 2$ .



**Fig. 4** In the same simple graph from earlier, we now only consider four nodes:  $m$  (origin),  $s$  (shelter), 3, 6 (refueling stations). The solid edges are the ones that we can use and correspond to the shortest paths that satisfy the fuel condition. The dashed edges are the ones that are unusable due to the fuel condition



**Fig. 5** The obtained shortest path that respects the fuel condition in both the new and original networks

**Step 3: Shortest Path Calculation**

The last step takes  $G^k$  and calculates a simple shortest path between the origin node  $m$  and the shelter  $s$ . The shortest path found is guaranteed to respect all refueling needs of vehicles of type  $k$  originating from node  $m$  (see Fig. 5).

### 3.3 Heuristic

For every vehicle fuel type  $k$ , we then calculate

$$\hat{b}_e^k = \sum_{i \in V: q_i^k > 0} \frac{\hat{\sigma}_{is}^k(e)}{\hat{\sigma}_{is}^k}, \quad (3)$$

where  $\hat{\sigma}_{is}^k$  is the number of side-constrained shortest paths connecting node  $i$  to  $s$  in  $G^k$  and  $\hat{\sigma}_{is}^k(e)$  is the number of those that also use edge  $e$ . Calculating this centrality value for every edge  $e$  will lead to a ranking of edges by importance for each vehicle fuel type  $k$ . The closer  $\hat{b}_e^k$  is to 1, the more important edge  $e$  is for vehicles of type  $k$  originating from node  $i$ . The metric can be easily updated into  $\hat{b}_e^{k'}$  to account for demands through multiplying by  $q_m^k$ , that is, using  $\hat{\sigma}_{mk}(e)' = q_m^k \cdot \hat{\sigma}_{mk}(e)$  in the numerator of (3). We actually use the metric that accounts for demands originating at each node in the heuristic, which consists of solving a simple knapsack problem as shown in (4). Since all “profits” of the knapsack problem are equal to one another, then the problem can be greedily solved by picking the  $B$  edges with highest  $\sum_{k \in K} \hat{b}_e^k$ .

$$\max \quad \sum_{e \in E} \sum_{k \in K} y_e \hat{b}_e^k \quad (4a)$$

$$s.t. \quad \sum_{e \in E} y_e \leq B, \quad (4b)$$

$$y_e \in \{0, 1\}, \forall e \in E. \quad (4c)$$

The full heuristic approach is presented in Algorithm 1. We note that it consists of three phases: in the first phase (lines 2–9), we consider the number of shortest paths and corresponding demands for each vehicle fuel type that passes through a specific node, subject to all refueling constraints. Then, in the second phase, we calculate the actual side-constrained betweenness metric (lines 10–16). Finally, in the third and last phase, we greedily solve a knapsack problem to identify the best edges to interrupt (lines 17–18). We note that in our implementation, the second phase can happen within the first phase loop; that said, for exposition purposes we present two loops for the two phases in Algorithm 1.

## 4 Computational Results

We show an indicative small case study on the transportation network of Sioux Falls, a well-known benchmark in transportation engineering [55]. We also use the demands and charging station locations as noted in the work of Purba et al. [11].

**Algorithm 1** Heuristic for identifying top  $B$  edges for disruption

---

```

1: function CRITICAL EDGES
2:   for all  $k \in K$  do
3:     for all  $m \in V : q_m^k > 0$  do
4:       Calculate  $\hat{\sigma}_{ms}^k$ 
5:       for all  $e = (i, j) \in E$  do
6:         Calculate  $\hat{\sigma}_{ms}^k(e)$ 
7:       end for
8:     end for
9:   end for
10:  for all  $k \in K$  do
11:    for all  $m \in V : q_m^k > 0$  do
12:      for all  $e = (i, j) \in E$  do
13:         $\hat{b}_e^{k'} \leftarrow q_m^k \cdot \hat{\sigma}_{ms}^k(e) / \hat{\sigma}_{ms}^k$ 
14:      end for
15:    end for
16:  end for
17:   $y^* \leftarrow \operatorname{argmax}_{y \in \{0,1\}^{|E|}} \left\{ \sum_{e \in E} \sum_{k \in K} y_e \hat{b}_e^k : \sum_{e \in E} y_e \leq B \right\}$ 
18:   $S \leftarrow \{e \in E : y_e^* = 1\}$ 
19:  return  $S$ 
20: end function

```

---

**Table 1** The roads that we should be protecting assuming  $R^2 = 2$

	$p$				
	1.0	0.75	0.50	0.25	0.00
Top #1	(5, 2)	(4, 2)	(4, 2)	(4, 2)	(4, 2)
Top #2	(9, 5)	(11, 4)	(11, 4)	(11, 4)	(11, 4)
Top #3	(4, 2)	(7, 2)	(7, 2)	(7, 2)	(10, 11)
Top #4	(7, 2)	(5, 2)	(18, 7)	(10, 11)	(7, 2)
Top #5	(11, 4)	(18, 7)	(20, 18)	(18, 7)	(18, 7)

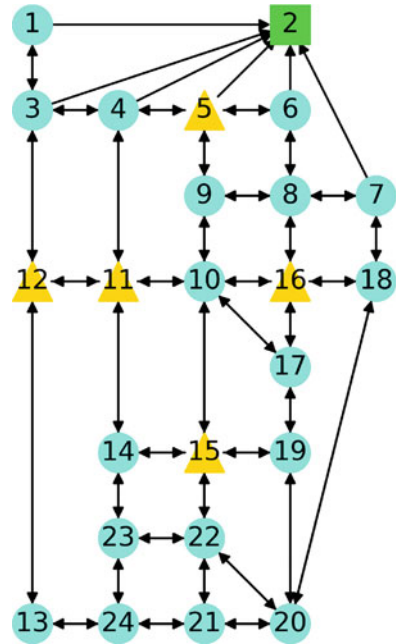
Specifically, our slightly modified network is shown in Fig. 6. The modification is due to the fact that node 2 that is designated as the shelter/safe zone is easy to disconnect in the original network; hence, we added more edges from nearby nodes. All the visualizations and the heuristic were implemented in Python using `networkx` [56].

Our experiment is designed as follows. First, we assume two different vehicle fuel types: the first one has enough fuel to traverse the network and escape without refueling and hence  $R^1 = M$ , while the second one has  $R^2 \in \{2, 3, 4\}$ . Then, we consider that the fraction of vehicles of fuel type 1 are  $p \in \{1, 0.75, 0.5, 0.25, 0\}$  (equivalently, the fraction of vehicles of fuel type 2 would be  $1 - p$ ). Finally, we try different values for the adversarial budget in  $B \in \{1, 2, 3, 4, 5\}$ . We note here that our heuristic approach will always be building on the previous solution. The edges that should be fortified/protected then are presented in Tables 1, 2, 3.

First of all, we observe that the results become more and more similar as the fuel capacity for vehicles of type 2 increases, becoming identical for  $R^2 = 4$ . We also



**Fig. 6** The network of the instance of Sioux Falls. The chargers for electric vehicles are in nodes 5, 11, 12, 15, and 16 (taken from [57]). The shelter/safety zone is at node 2. A change from the original network is that edges have been added from nodes 3, 4, 5, and 7 toward safety



**Table 2** The roads that we should be protecting assuming  $R^2 = 3$

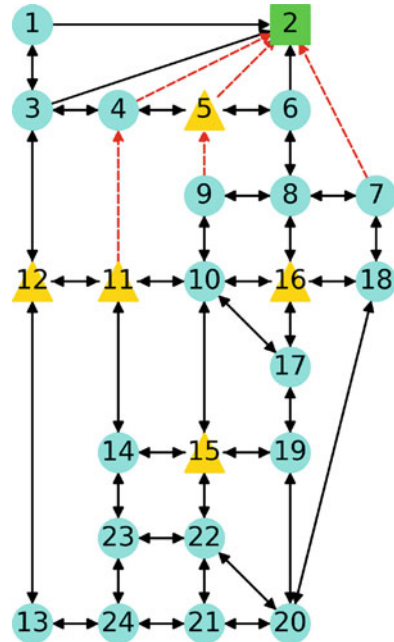
	$p$				
	1.0	0.75	0.50	0.25	0.00
Top #1	(5, 2)	(4, 2)	(4, 2)	(4, 2)	(4, 2)
Top #2	(9, 5)	(5, 2)	(11, 4)	(11, 4)	(11, 4)
Top #3	(4, 2)	(11, 4)	(5, 2)	(5, 2)	(6, 2)
Top #4	(7, 2)	(9, 5)	(9, 5)	(6, 2)	(5, 2)
Top #5	(11, 4)	(7, 2)	(6, 2)	(9, 5)	(8, 6)

**Table 3** The roads that we should be protecting assuming  $R^2 = 4$

	$p$				
	1.0	0.75	0.50	0.25	0.00
Top #1	(5, 2)	(5, 2)	(5, 2)	(5, 2)	(5, 2)
Top #2	(9, 5)	(9, 5)	(9, 5)	(9, 5)	(9, 5)
Top #3	(4, 2)	(4, 2)	(4, 2)	(4, 2)	(4, 2)
Top #4	(7, 2)	(7, 2)	(7, 2)	(7, 2)	(7, 2)
Top #5	(11, 4)	(11, 4)	(11, 4)	(11, 4)	(11, 4)

observe that as the distribution of vehicles changes, and the alternative fuel vehicles (vehicles of type 2) increase in number, then the adversary starts attacking more roads in the periphery so as to hurt access to refueling infrastructure. On the other hand, when only conventional vehicles are on the road, then the adversary focuses their attacks on the roads leading to the shelter.

**Fig. 7** The solution obtained for a budget of five attacks in the case where  $R^2 = 4$



As we noted earlier, the results for  $R^2 = 4$  are identical, no matter the distribution of vehicles. This is expected as  $R^2 = 4$  is big enough in this network for the two vehicles to evacuate following similar routes. We show the solution obtained in all distributions for  $R^2 = 4$  in Fig. 7.

## 5 Concluding Remarks

In this work, we build upon previous work in evacuation planning with and without alternative fuel vehicles. Newer technology vehicles that are powered by electricity or hydrogen are becoming more and more popular; that said, they also come with the setback of having sparser refueling infrastructure available to them. Due to that, they can become particularly vulnerable during a large-scale evacuation order. Additionally, the dependence of our transportation infrastructure on electricity and communication networks renders it more susceptible to cyberattacks. Hence, a hybrid threat in the form of a natural disaster (e.g., hurricane) and a terrorist attack (e.g., cyberattack or misinformation campaign) can be treacherous for all evacuees and more so for evacuees relying on alternative fuel vehicles.

This is why we propose an evacuation modeling framework that considers the refueling needs of alternative fuel vehicles alongside more traditional vehicles. We also propose a new framework that reveals the biggest gaps in our evacuation plans:

specifically, we ask the question, “What is the set of roads that are most critical for the success of the evacuation?” Due to the difficulty of the bilevel problem proposed, we design and implement a variant of the betweenness centrality metric and we use it in a heuristic to identify the most critical edges in our transportation network. We conclude this work with the presentation of results of numerical experiments in a small-scale network. We show that both the distribution of vehicles in the market and the fuel capacity (driving range) of vehicles affects the evacuation plan and the attack strategy of the adversary.

Extensions of this work should focus on exact or heuristic solution methodologies of the proposed bilevel problem addressing the criticality of links of the evacuation networks of alternative fuel vehicles. Additionally, a comparison between other centrality metrics in the context of criticality in the presence of alternative fuel vehicles in a transportation network would be useful. Future research can leverage our work on hybrid threats to create fortification plans of evacuation and alternative fuel infrastructure networks. The siting of refueling infrastructure networks can be modeled to address both cost efficiency and resilience of a transportation system powered by a diversity of sources.

**Acknowledgments** This research is part of the Blue Waters sustained-petascale computing project, which is supported by the National Science Foundation (awards OCI-0725070 and ACI-1238993), the state of Illinois, and the National Geospatial-Intelligence Agency. Blue Waters is a joint effort of the University of Illinois at Urbana-Champaign, its National Center for Supercomputing Applications, and the UIUC Office of the Vice Chancellor of Research and Innovation’s New Frontiers Initiative.

## References

1. Hardman, S., Chandan, A., Tal, G., Turrentine, T.: The effectiveness of financial purchase incentives for battery electric vehicles—a review of the evidence. *Renew. Sustain. Ener. Rev.* **80**, 1100–1111 (2017)
2. Funke, S. Á., Sprei, F., Gnann, T., Plötz, P.: How much charging infrastructure do electric vehicles need? a review of the evidence and international comparison. *Transp. Res. D Transp. Environ.* **77**, 224–242 (2019)
3. Wu, Y.-C., Kontou, E.: Designing electric vehicle incentives to meet emission reduction targets. *Transp. Res. D Transp. Environ.* **107**, 103320 (2022)
4. New York Times: President Biden sets a goal of 50 percent electric vehicle sales by 2030. <https://www.nytimes.com/2021/08/05/business/biden-electric-vehicles.html>. Accessed: 2022-06-13
5. Department of Energy: Fact of the Week: Model Year 2021 All-Electric Vehicles Had a Median Driving Range about 60% That of Gasoline Powered Vehicles. <https://www.energy.gov/eere/vehicles/articles/fotw-1221-january-17-2022-model-year-2021-all-electric-vehicles-had-median>. Accessed: 2022-06-13
6. Mashayekh, Y., Jaramillo, P., Samaras, C., Hendrickson, C.T., Blackhurst, M., MacLean, H.L., Matthews, H.S.: Potentials for sustainable transportation in cities to alleviate climate change impacts. *Environ. Sci. Technol.* **46**(5), 2529–2537 (2012)
7. Feng, K., Lin, N., Xian, S., Chester, M.V.: Can we evacuate from hurricanes with electric vehicles? *Transp. Res. D Transp. Environ.* **86**, 102458 (2020)

8. Adderly, S.A., Manukian, D., Sullivan, T.D., Son, M.: Electric vehicles and natural disaster policy implications. *Energy Policy* **112**, 437–448 (2018)
9. Li, Q., Soleimaniamiri, S., Li, X.: Optimal mass evacuation planning for electric vehicles before natural disasters. *Transp. Res. D Transp. Environ.* **107**, 103292 (2022)
10. MacDonald, C.D., Kattan, L., Layzell, D.: Modelling electric vehicle charging network capacity and performance during short-notice evacuations. *Int. J. Disaster Risk Reduct.* **56**, 102093 (2021)
11. Purba, D.S.D., Kontou, E., Vogiatzis, C.: Evacuation route planning for alternative fuel vehicles. *Transp. Res. Part C Emerg. Technol.* **143**, 103837 (2022). <https://doi.org/10.1016/j.trc.2022.103837>
12. Murray-Tuite, P., Wolshon, B.: Evacuation transportation modeling: An overview of research, development, and practice. *Transp. Res. C Emerg. Technol.* **27**, 25–45 (2013)
13. Lindell, M.K., Murray-Tuite, P., Wolshon, B., Baker, E.J.: *Large-scale Evacuation: The Analysis, Modeling, and Management of Emergency Relocation from Hazardous Areas*. CRC Press, New York, NY (2018)
14. Kim, S., George, B., Shekhar, S.: Evacuation route planning: scalable heuristics. In: *Proceedings of the 15th Annual ACM International Symposium on Advances in Geographic Information Systems*, pp. 1–8 (2007)
15. Lim, G.J., Zangeneh, S., Baharmemati, M.R., Assavapokee, T.: A capacitated network flow optimization approach for short notice evacuation planning. *Eur. J. Oper. Res.* **223**(1), 234–245 (2012)
16. Vogiatzis, C., Walteros, J.L., Pardalos, P.M.: Evacuation through clustering techniques. In: Goldengorin, B., Kalyagin, V.A., Pardalos, P.M. (eds.) *Models, Algorithms, and Technologies for Network Analysis*, pp. 185–198. Springer, New York, NY (2013)
17. Andreas, A.K., Smith, J.C.: Decomposition algorithms for the design of a nonsimultaneous capacitated evacuation tree network. *Netw. Int. J.* **53**(2), 91–103 (2009)
18. Achrekar, O., Vogiatzis, C.: Evacuation trees with contra flow and divergence considerations. In: *International Conference on Dynamics of Disasters*, pp. 1–46. Springer, New York (2017)
19. Kim, S., Shekhar, S., Min, M.: Contra flow transportation network reconfiguration for evacuation route planning. *IEEE Trans. Knowl. Data Eng.* **20**(8), 1115–1129 (2008)
20. Gao, Y., Chiu, Y.-C., Wang, S., Küçükyavuz, S.: Optimal refueling station location and supply planning for hurricane evacuation. *Transp. Res. Rec.* **2196**(1), 56–64 (2010)
21. Department of Homeland Security: Sector risk snapshots. <https://www.hsdil.org/?abstract&did=754033>. Accessed: 2022-05-31
22. Lehto, M.: In: Lehto, M., Neittaanmäki, P. (eds.) *Cyber-Attacks Against Critical Infrastructure*, pp. 3–42. Springer, Cham (2022). <https://doi.org/10.1007/978-3-030-91293-21>
23. Walteros, J.L., Pardalos, P.M.: Selected topics in critical element detection. *Appl. Math. Inf. Military Sci.*, 9–26 (2012)
24. Lalou, M., Tahraoui, M.A., Kheddouci, H.: The critical node detection problem in networks: A survey. *Comput. Sci. Rev.* **28**, 92–117 (2018)
25. Lewis, J.M., Yannakakis, M.: The node-deletion problem for hereditary properties is np-complete. *J. Comput. Syst. Sci.* **20**(2), 219–230 (1980)
26. Wan, Z., Mahajan, Y., Kang, B.W., Moore, T.J., Cho, J.-H.: A survey on centrality metrics and their network resilience analysis. *IEEE Access* **9**, 104773–104819 (2021)
27. Jeong, H., Mason, S.P., Barabási, A.-L., Oltvai, Z.N.: Lethality and centrality in protein networks. *Nature* **411**(6833), 41–42 (2001)
28. Hahn, M.W., Kern, A.D.: Comparative genomics of centrality and essentiality in three eukaryotic protein-interaction networks. *Mol. Biol. Evol.* **22**(4), 803–806 (2005)
29. Yoon, J., Blumer, A., Lee, K.: An algorithm for modularity analysis of directed and weighted biological networks based on edge-betweenness centrality. *Bioinformatics* **22**(24), 3106–3108 (2006)
30. Russo, T.C., Koesten, J.: Prestige, centrality, and learning: A social network analysis of an online class. *Commun. Educ.* **54**(3), 254–261 (2005)

31. Vogiatzis, C., Teixeira-Poit, S.M., Walton, T.N., Gowdy, G., Ram, B.: Research engineer network: A network analysis of graduate student relationships. In: 2021 ASEE Virtual Annual Conference Content Access (2021)
32. Borgatti, S.P., Mehra, A., Brass, D.J., Labianca, G.: Network analysis in the social sciences. *Science* **323**(5916), 892–895 (2009)
33. Duijn, P.A., Klerks, P.P.: Social network analysis applied to criminal networks: recent developments in dutch law enforcement. *Netw. Netw. Anal. Defence Secur.*, 121–159 (2014)
34. Derrible, S.: Network centrality of metro systems. *PLOS ONE* **7**(7), 1–10 (2012). <https://doi.org/10.1371/journal.pone.0040575>
35. Guimera, R., Mossa, S., Turtschi, A., Amaral, L.N.: The worldwide air transportation network: Anomalous centrality, community structure, and cities' global roles. *Proc. Natl. Acad. Sci.* **102**(22), 7794–7799 (2005)
36. Fleming, D.K., Hayuth, Y.: Spatial characteristics of transportation hubs: centrality and intermediacy. *J. Transp. Geogr.* **2**(1), 3–18 (1994)
37. Bavelas, A.: A mathematical model for group structures. *Hum. organ.* **7**(3), 16–30 (1948)
38. Bavelas, A.: Communication patterns in task-oriented groups. *J. Acoust. Soc. Am.* **22**(6), 725–730 (1950)
39. Anthonisse, J.M.: The rush in a directed graph. *Stichting Mathematisch Centrum. Mathematische Besliskunde (BN 9/71)* (1971)
40. Freeman, L.C.: A set of measures of centrality based on betweenness. *Sociometry*, 35–41 (1977)
41. Freeman, L.C.: Centrality in social networks conceptual clarification. *Soc. Netw.* **1**(3), 215–239 (1978)
42. Dangalchev, C.: Residual closeness in networks. *Phys. A Stat. Mech. Appl.* **365**(2), 556–564 (2006)
43. Everett, M.G., Borgatti, S.P.: The centrality of groups and classes. *J. Math. Sociol.* **23**(3), 181–201 (1999)
44. Everett, M.G., Borgatti, S.P.: Extending centrality. *Mod. Methods Soc. Netw. Anal.* **35**(1), 57–76 (2005)
45. Veremyev, A., Prokopyev, O.A., Pasiliao, E.L.: Finding groups with maximum betweenness centrality. *Optim. Methods Softw.* **32**(2), 369–399 (2017)
46. Vogiatzis, C., Veremyev, A., Pasiliao, E.L., Pardalos, P.M.: An integer programming approach for finding the most and the least central cliques. *Optim. Lett.* **9**(4), 615–633 (2015)
47. Rysz, M., Pajouh, F.M., Pasiliao, E.L.: Finding clique clusters with the highest betweenness centrality. *Eur. J. Oper. Res.* **271**(1), 155–164 (2018)
48. Vogiatzis, C., Camur, M.C.: Identification of essential proteins using induced stars in protein–protein interaction networks. *INFORMS J. Comput.* **31**(4), 703–718 (2019)
49. Camur, M.C., Sharkey, T., Vogiatzis, C.: The star degree centrality problem: A decomposition approach. *INFORMS J. Comput.* **34**(1), 93–112 (2022)
50. Rasti, S., Vogiatzis, C.: Novel centrality metrics for studying essentiality in protein–protein interaction networks based on group structures. *Networks* (2021). <https://doi.org/10.1002/net.22071>
51. Vogiatzis, C., Pardalos, P.M.: Evacuation modeling and betweenness centrality. In: *International Conference on Dynamics of Disasters*, pp. 345–359. Springer (2016)
52. Lujak, M., Giordani, S.: Centrality measures for evacuation: Finding agile evacuation routes. *Future Gener. Comput. Syst.* **83**, 401–412 (2018)
53. Brandes, U.: A faster algorithm for betweenness centrality. *J. Math. Sociol.* **25**(2), 163–177 (2001)
54. Barthelemy, M.: Betweenness centrality in large complex networks. *Eur. Phys. J. B* **38**(2), 163–168 (2004)

55. Transportation Networks for Research Core Team: Transportation Networks for Research. Accessed: 2022-05-31. <https://github.com/bstabler/TransportationNetworks>
56. Hagberg, A., Swart, P., S Chult, D.: Exploring network structure, dynamics, and function using networkx. Technical report, Los Alamos National Lab.(LANL), Los Alamos, NM (United States) (2008)
57. He, F., Yin, Y., Lawphongpanich, S.: Network equilibrium models with battery electric vehicles. *Transp. Res. B Methodol.* **67**, 306–319 (2014)

# Risk Assessment and Identification Methodology for the Defense Industry in Times of Crisis: Decision-Making



Isabella T. Sanders

## 1 Introduction

Supply chains are only as strong as the connections within them. One of the key bonds in a supply chain is the relationship between a firm and its supplier. A firm depends on its suppliers for reliability. A single plant shutdown can cause disruptions throughout the supply chain costing companies time and money. It is important to be able to assess risk in a supply chain in order to inform firms of potential weak links. In fact, a reduced supplier base is one of the main factors contributing to potential supply chain disruptions [11]. In times of crisis, the factors that contribute to supplier risk are often exaggerated but not any different than in normal times. A robust risk model will include factors that measure risks for such crises.

Some risks are routine and easily predictable, and others are not as easily forecasted. Therefore, supply chain risk can often be hard to quantify and subjective. Historical methods to assess supply chain risk in applied situations often involve a high degree of subjectivity with a focus on qualitative information. This study's risk assessment computes supplier risk by concentrating on the use of quantitative data. Suppliers face risk from many different directions.

U.S. government purchasing agents oversee complex and elaborate supply chains. Each purchasing agent oversees thousands of contract companies with tens of thousands of plants. Such complexity within supply chains can be tough to manage [27]. With such an expansive supply chain, it can be difficult to screen potential and existing suppliers using historical methods that focus on time-intensive qualitative data collection through the use of interviews and surveys. The US

---

I. T. Sanders (✉)

Department of Systems Engineering, United States Military Academy, West Point, NY, USA  
e-mail: [isabella.sanders@westpoint.edu](mailto:isabella.sanders@westpoint.edu)

government has studied the potential use of bankruptcy models but concluded that at the time of publishing there was not a promising strategy [8]. The US government also has created risk models, but found that some factor definitions are too ambiguous and some factors are hard to obtain [42]. Our model aims to present a clear data-driven framework that quantifies supplier risk at the plant level through a combination and weighting of different metrics.

## 2 Literature Review

The supply chain risk management (SCRM) field gained traction in the early 2000s and has grown to interlap with other directly related areas such as enterprise risk management and supply chain management [43]. SCRM “encompasses the collaborative and coordinated efforts of all parties involved in a supply chain to identify, assess, mitigate and monitor risks with the aim to reduce vulnerability and increase robustness and resilience of the supply chain, ensuring profitability and continuity” [4]. There are three main techniques to model and solve problems within SCRM, “(1) multiple criteria decision analysis techniques; (2) mathematical modeling and optimization; and (3) Artificial Intelligence (AI) techniques” [3]. This paper chooses to focus on the supplier risk identification and assessment stages of SCRM using multiple criteria decision analysis techniques and mathematical modeling to model and solve.

Supply risk is made up of all risk that arises due to the disruption of upstream movement of materials, information, or capital [35]. Eberle [15] breaks supply risk into two categories, external procurement risks and internal operational risks. A later paper studied the significance of both internal and external procurement risks and found that external procurement risks from the supply side make up the largest threat within industry [24]. Here, we focus specifically on Supplier Risk Identification and Assessment.

## 3 Supplier Risk Classifications

Several studies have broken down supply risk into different classifications with different weights. Mason-Jones and Towill [28] break risk into overlapping categories of environmental, supply and demand, process risk, and control risk. Zsidisin [54] focuses on internal supply risks including design, quality, cost, availability, manufacturability, supplier, legal, and environmental health and safety. Matook [29] assesses each supplier based on seven risk types price, quality, quantity, process, technology, economic, and environmental. Pettit’s [36] Supply Chain Resilience Framework identifies seven different sources of supply chain vulnerability: turbulence, deliberate threats, external pressures, resource limits, sensitivity, connectivity, and supplier/customer disruptions. There have also been studies done focusing



on specific industries. Blackhurst [7] focuses on the automotive industry where risk is assessed at the part level in the overarching categories of quality and disruptions/disasters. Sinha et al. [41] focused on the aerospace industry studying the difference between foreseen and perceived risks where a foreseen risk is backed by data and a perceived risk is identified based on intuition and speculation.

Risk weights within these studies are either not discussed [36] or determined by either the researchers [7], or statistical analysis ([23, 29]). We propose the use of an established technique that has not been used in supply chain risk literature to our knowledge, the DELPHI method. The method was first introduced in a study conducted by the RAND Corporation with sponsorship by the US Air Force. The DELPHI method combines the decisions of a structured group of individuals through a series of rounds of questionnaires in order to “obtain the most reliable consensus of opinion of a group of experts” [13]. Since its inception, it has been successfully used in the fields including but not limited to location analysis [25], business forecasting [21], and food risk governance [52]. The DELPHI method is used in this study to collect the risk factors influencing the supply chain, select the appropriate factors, and weigh each of the factors. Since there is little literature on supply chain risk for government purchasers, the Delphi method will enable this study to ensure a comprehensive list of risk factors is considered for selection and appropriate weights are carefully chosen.

Every supply chain is unique and a subset of risk metrics should be chosen based on the firm, not a compiled exhaustive list. “There is no ‘one size fits all’ approach to assessing risk” firms “need to define risk categories based upon their own needs, industry type, supply chain type” [7]. Risk identification and assessments must align with the supply chain objectives of the firm [29]. A reduced number of risk categories is favored such that the amount of data needed is lessened [29] resulting in a model that is easy to understand and implement. Therefore, in this study we choose a subset of vulnerabilities from these authors in which to build our supplier risk model and expand certain categories to address particular risks present within US Government Developer supply chains.

The literature presents conceptual frameworks [36], an analysis of current techniques [53], and proposed risk assessment models with limited implementation [7, 37, 41]. These previous works depend on the use of surveys, focus groups, observations, and interviews for implementation, focusing on qualitative information. While valuable, gathering this information can be time-intensive and the information gathered is often subjective. Blackhurst et al. [7] call for future research to “explore the use of intelligent agents to automatically collect and enter some of the data required to use the model.” This paper aims to create a data-driven model where the majority of information originates from scientific data sources, which can be routinely pulled from online databases and sources through a computer program. This data-centric approach reduces the bias within the model associated with human error and allows for accelerated information collection and input into the model. Accelerated information collection leads to a swifter model execution time frame enabling firms to run the model more often and assess risk regularly.

## 4 Financial Bankruptcy

Financial risk is an important consideration within supplier risk and has been used in numerous studies. The U.S. bankruptcy code consists of five principal chapters, with the two most predominant chapters being chapter seven (liquidation) and chapter eleven (reorganization of a business). The most common form of bankruptcy in the U.S. is chapter seven bankruptcy [49]. However, within U.S. Government Purchasers chapter eleven is more common [19]. In this study, we consider both chapter seven and chapter eleven bankruptcy.

Bankruptcy models have been studied for many years [1, 5, 33]. However, they are seldom used within supplier risk models. The proposed classification model will often include a financial/bankruptcy risk factor but will not explore the calculation of this factor. Within supplier risk classifications, bankruptcy risk is often treated as a black box where the risk rating is determined by the subjective judgment of a manager without any supporting data provided. Matook et al. [29] used a combination of questionnaires and expert discussions to determine their economic risk factor. Blakhurst et al. [7] allowed “ratings for [risk] factors [to] be made by purchasing agents, production control personnel, quality inspectors production level employees, etc.” While these employees may be familiar with their plants and even risk assessment, this method leaves room for a great degree of subjectivity. Each employee views risk from their own lens where a risk of 7 for one employee may be 9 for another. While subjectivity is likely to always be present within supplier risk models, it is important to limit it as much as possible to reduce bias. Jung et al. [23] is one of the few studies that utilizes data-supported financial factors proven effective by previous bankruptcy studies within their supply risk analysis but is not focused on the defense industry.

There have been dozens of bankruptcy models proposed in literature over the past 60 years. Historical models have used hundreds of different factors in different combinations [6]. Examples of such factors include financial ratios [1], market-based variables [9, 40], and macroeconomic variables [47]. The four main model types found in bankruptcy literature include discriminant analysis, logit analysis, probit analysis, and neural networks [6]. Even with a great amount of differences existing between models in the literature, the majority of these models “show high predictive ability” in empirical testing [6]. Despite the abundance of models available, bankruptcy prediction models are not commonly used in practice or in supplier risk analyses. Bellovary et al. [6] call for future research to focus on the use and application of existing models rather than the creation of new models. Therefore, we expand upon the work done by Dickerson et al. [14], which builds a linear discriminant bankruptcy model that is trained, validated, and tested on a novel defense sample dataset. In their study, they compared the performance of their own model to well-known military bankruptcy models of Dagele and Pepper [12], Moses and Liao [31], Godfrey [20] and the most popular general bankruptcy models in literature Ohlson [33] and Altman [1]. As Dickerson et al.’s model has the best efficacy as applied to the most recent decent data at 92%, it is used in our hybrid

risk assessment model within the financial risk category of the overall supplier risk assessment.

Very few empirical studies exist that consider both financial indicators and other supplier risk indices [23]. Jung et al. [23] present a study that considers suppliers (at the company level) of a purchasing agent, which focuses on mostly internal risk factors. The study considers supplier risk, market, switching, relationship, list, size, quality, technology, delivery, and cost in addition to financial variables used in previous bankruptcy studies. The financial and cost capability variables that were calculated from the financial information of suppliers and quality, dependability, and R&D capabilities were estimated based on internal agent data. Jung produces a valuable framework for supplier risk management. However, the needs and concerns of a large-scale US government purchaser are different than that of a Fortune 500 Korean firm leading us to present a new framework.

Our study explores supplier risk at the plant level, a step deeper than the company or firm level. In addition, this paper introduces several location-based risk factors accounting for the geographical spread of the suppliers. Through integrating financial, internal, and location-based risk factors at a global level, we address both Jung and Bellovary's suggestions for future research and create a novel data-based structured model for global suppliers.

## 5 Summary of Model

Most historical supply chain risk models have been built on qualitative data and do not explore the data collection necessary to implement the model. When empirical studies are done, the models depend on time-consuming qualitative data collection. Very few empirical studies exist that utilize existing bankruptcy models to incorporate financial risk into the supplier risk methodology. Though the US government has built risk models before, there is a current need for a structured, data-driven supplier risk methodology that is easily implemented. Our framework uses the DELPHI method for risk factor selection and weight. The values of the factors for each plant are retrieved from reputable quantitative data sources. Specifically, the financial outlook risk factor is supported by a proven model in bankruptcy literature. This methodology is then implemented through a case study of a US government aerospace developer to assess the risk of a sample of its suppliers, which includes dozens of firms made up of over 600 domestic and foreign plants.

## 6 Methodology

Our objective is to create a data-driven supplier risk model that can assess risk within supply chains in defense. The model classifies each supplier plant as either good,

watch, or alert. Each year, purchasers must determine which contracts to renew and which new contracts to accept. A classification of watch or alert signals the purchaser to conduct further research on risky firms, before signing an agreement. This classification model helps to reduce the number of firms to be further examined, by identifying particularly risky ones, saving time. Informed decision-making empowered by this model can improve the stability of a purchaser's supplier base. We consider several factors in this supplier risk assessment. Multicriteria scoring approaches are commonly used for decision-making in conditions where several factors must be considered for final output [7]. Therefore, our risk assessment model is built using a multicriteria scoring approach to develop risk indices at the plant level. We then apply our model to a sample of US government suppliers within the aerospace industry.

## 7 Application of the DELPHI Method

The first step in the methodology is to establish a list of the most important risk factors within the defense industry. We choose to gather and decide these factors through the use of the DELPHI method to combine the input of several experts [13]. The experiment consisted of surveying a panel of six experts within Government and Academia. These experts included two branch chiefs, an academic well-versed in supply chain risk, and SMEs in the subjects of Supply Chain, Lean Six Sigma, and Materials. A series of four questionnaires were submitted on a staggered basis. Interviews were conducted for any follow-up questions. The experts were given the following premise as the base of the experiment (Exhibit 1).

**Summary of Project** This study is to create a global supplier risk assessment model for US government purchasers specifically within the defense industry. This risk assessment model is intended to be used annually to assess the risk of suppliers to the Government at the CAGE (plant) Level in order to renew and establish contracts. In an effort to make the risk assessment as accurate as possible, we are employing the DELPHI model in order to choose the best weights for the risk factors within the model. We seek your expertise as a branch chief, team lead, or SME to add input into the weightings of our risk categories. To capture the spirit of the experiment, summaries of each questionnaire and research actions taken in between can be seen (Exhibits 2, 3, and 4) as follows:

## 8 Risk Factors

The following risk components were selected during the DELPHI risk study. The components were grouped into categories by the authors based on earlier supply chain risk literature where possible. Each risk component and category is given a

**Questionnaire 1:**

Considering the summary of project you were given, based on your own experience, please list the factors that you believe should be considered for incorporation in this model.

**Researcher Action:**

Researchers examined all the factors and created categories such that every factor could be grouped into a category. Categories were pulled from literature in supply chain risk where possible. No factors were eliminated and categories were given definitions for experts.

**Questionnaire 2:**

Based on the first round of questionnaires and interviews there were risk components in 9 main categories that were suggested. These categories and components were given to experts as a reference which can be seen in Figure 1. Experts were then asked to review these categories and components and add any components they believed to be missing. Once experts believed they had an exhaustive list, they were asked to examine each component and indicate whether they believed the component had a reliable and easily found data source. If so, they were asked to list the source.

**Researcher Action:**

Researchers took in the responses of the experts and spent time identifying data sources for each component if possible. Components where data sources could not easily be found after extensive research and/or were not able to be collected in a three-month time frame were identified by the researchers. Weighing the costs and benefits, the researchers decided that it would be too time intensive to try and gather data for these components and removed them from this data-driven study. Removal does not indicate that these factors could not have been potentially useful. The goal of this study is to create an *easily implementable* model for government purchasers that can be adapted to other fields. A model that is easily implementable must include quick data collection.

**Questionnaire 3:**

Experts were given the revised list of categories and components as seen in Figure 2. They were given definitions of categories and components in addition to data sources for examination. They were asked to identify any components they believed to be unimportant to supplier risk.

**Researcher Action:**

No categories or components were identified so no action was taken.

**Questionnaire 4:**

Experts were then given the same chart they were given in Questionnaire 3, which lists the pertinent risk categories and components. For each category with multiple components they were asked to weight the importance of each component to the overall category from 0-100 such that the weights summed to 100. They were then asked to weight the importance each categories to the overall supplier risk from 0-100 such that the sum of all of the category weights added up to 100. Example tables that were given to the experts can be seen in Figure 3.

**Researcher Action:**

The weights from each expert were compiled and averages for all components and categories were tabulated which can be seen in Figure 4. These weights are later used within the multi-criteria scoring model.

**Exhibit 1** Outline of interviews

score from 0 to 5 based on available data, where 0 indicates the lowest risk and 5 indicates the highest risk. High risk, or a rating of 4–5, for any category or in the overall rating indicates that the purchaser should further research the firm for more specific sources of that risk to make a more educated purchasing decision.

## 9 Turbulence

Turbulence is defined as an “environment characterized by frequent changes in external factors beyond [company] control” by Pettit [36]. In this methodology, turbulence is divided into two components: natural hazards and disasters and

Turbulence	Deliberate Threat	Financial Risk	Foreign Dependence	Firms in Sector	DOD Dependence	Performance	Criticality	Firm Exiting Industry
Environment characterized by frequent changes in external factors beyond company control.	Intentional Attacks aimed at disrupting operations or causing human or financial harm.	Chance of bankruptcy.	What is the dependence on foreign sources for this capability?	How many firms currently participate in this firm's market for this capability?	What percentage of company sales are DOD sales?	How does the company perform on current contracts?	Characteristics that make a specific product or service difficult to replace if disrupted	Chance that the firm/plant will exit the industry stop operating.
Natural Disasters	Theft	Accounting ratios	Preferred Suppliers	Active Producers Available	Too much dependence on DOD	Late Payment	Defense unique	Diversity of products
Geopolitical Disruptions	Terrorism	Market Variables	Resource Constraints	AP already Army customers	Too little dependence on DOD	Late Delivery	Facility & Equipment Requirements	
Unpredictability of Demand	Labor Disputes	Legal Issues				Defects/million	Defense Design Requirements	
Pandemic	Espionage					Poor Quality	Skilled Labor	
Legal Issues							Reconstitution Time	
							Availability of Alternatives	

Exhibit 2 Round table 1 summary

Risk Criterion	Component	Country	Scale	Data Title	Data Source
Turbulence	Natural Disasters	USA	County	US Natural Hazards Index	National Center for Disaster Preparedness at Columbia University
Turbulence	Natural Disasters	Foreign	Country	Global Climate Risk Index	Germanwatch
Turbulence	Geopolitical Disruptions	All	Country	Political Risk Map	Marsh
Deliberate Threat	Terrorism	ALL	Country	Global Terrorism Index	Institute for Economics & Peace and National Consortium for the Study of Terrorism & Responses to Terrorism at US Department of Homeland Security
Deliberate Threat	Labor Disputes	USA	State	US Work Stoppages	US Bureau of Labor Statistics
Deliberate Threat	Labor Disputes	Europe	Country	ETUI Strikes Map	The European Trade Union Institute financially Supported by the European Union
Deliberate Threat	Labor Disputes	Canada	Country	Canada Work Stoppages	Employment and Social Development Canada, the Government of Canada
Deliberate Threat	Labor Disputes	Australia	Country	Australia Industrial Disputes	Australian Bureau of Statistics, the Australia Institute Centre for Future Work
Deliberate Threat	Labor Disputes	USA	State	Right to Work Laws	National Right to Work Committee
Financial Risk	Dickerson et al. Model	USA	Firm	Financial Data	Wharton Research Data Services (COMPUSTAT), Yahoo Finance, S&P Global Capital IQ
Foreign Influence	Human Rights Laws	ALL	Country	Human Rights Laws	Fund for Peace
Foreign Influence	Conflict Minerals	ALL	Country	Conflict Minerals	SEC
Foreign Influence	Foreign Entity	ALL	Country	N/A	N/A
DoD Dependence	DoD dependence	USA	Firm	DoD Dependence	SEC (10Q) and Company Annual Reports

Exhibit 3 Risk criterion and components

geopolitical disruptions. *Natural hazards* are defined as a natural phenomenon that has potential for an adverse effect on humans [34]. A *natural disaster* is a hazardous event caused by natural hazards, which results in injuries, fatalities, and/or property damage [34]. *Geopolitical disruptions* are changes that result from government influence such as currency inconvertibility, trade embargoes, seizure of assets by host governments, and political violence [26].

Natural disasters and geopolitical disruptions are extremely important for suppliers to consider when evaluating risk. A single disaster or disruption can cause delays in multiple plants at the same time. For example, in 2005 Hurricane Rita hit Texas and Louisiana hard, resulting in shutdowns of many oil refining assets throughout the area. Consumer-packaged goods firms were reliant on raw materials from these

<b>Sample Survey</b>	
Risk Criterion Ratings	Your Estimate
Turbulence	
Deliberate Threat	
Financial Risk	
Foreign Dependence	
DoD Dependence	
<b>Sum</b>	100

**Exhibit 4** Sample survey

suppliers for their petroleum-based packaging. Shutdowns greatly impacted these firms and caused many to change the materials for their packaging [38]. The turbulence category is not unique to Pettit and similar categories can be seen in numerous papers, demonstrating its importance, including a “disruptions/disaster” category [7], an “environmental risk” [29], and a “disasters” category [53]. Three different data sources were used for the turbulence category in our methodology.

Natural hazards and disasters *domestic* data were taken from the U.S. Natural Hazards Index created by the Natural Center for Disaster Preparedness at Columbia University. The index uses historical and projected aggregated data from eleven individual disaster categories: wildfire, volcano, tornado, snowfall, landslide, hurricane, earthquake, drought, heat wave, avalanche, and flood [10]. These data are found at the county level and are assigned to CAGES by their location. Natural hazards and disasters *foreign* data were taken from the Global Climate Risk Index (GCRI) created by Germanwatch. The GCRI calculates an index for each country and bases its analysis on data sets that measure the impacts of historical extreme weather events [16]. It focuses on extreme weather events rather than slow-onset processes such as global warming. Though these data sources are slightly different, both indices are founded on reliable data. Domestic and foreign ratings were calculated on separate scales due to the difference in the indices, but the end rating can be compared from country to country.

The geopolitical disruptions’ domestic and foreign data were taken from the same source, the Political Risk Map 2020 created by Marsh, a global insurance broker and risk advisor. Marsh annually completes a Political Risk Map Report where the scores are calculated at the country level. In this Political Risk Map, “the overall risk scores are based on three categories of risk—political, economic, and operational—and reflect both short- and long-term threats to stability” [26].



## 10 Deliberate Threat

Deliberate threats are defined as “intentional attacks aimed at disrupting operations or causing human or financial harm” by Pettit [36]. In this framework, the deliberate threat is broken into terrorism and labor disputes. *Terrorism* is defined as “the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation” [22]. Labor disputes are characterized by disagreements between a firm and its employees based on conditions of employment. In this study, we are looking at the subset of labor disputes that become work stoppages or strikes where there is a cessation of work by employees. Few papers use a category similar to the deliberate threat. Blackhurst et al. use a war/terrorism component within the “disruptions/disaster” category and mention the importance of strikes in their introduction [7]. Despite its rarity in literature, both terrorism and labor disputes were noted clearly by experts in our DELPHI study and they are essential factors within supply chain risk.

Deliberate threats have always been a risk to businesses. Work stoppages harm business in an obvious way, and man-hours or often days are lost due to employee/union protest. This can delay production and impact other parts of the supply chain. Terrorism is a growing threat to supply chains. According to the Material Handling and Logistics, in 2016, 346 terrorist attacks took place in a wide variety of industries and modes of transport. There are many indirect and direct costs as a result of terrorism attacks on supply chains including physical damage and rerouting shipping flows [30].

Labor dispute data were taken from several different sources. European data were compiled from the European Trade Union Institute, which is financially supported by the European Union [51]. ETUI provides a booklet, which contains summary statistics concerning strikes in most European countries. We use the average days not worked due to industrial action per 1000 employees from 2010 to 2018. For Canadian data, we use data from the Employment and Social Development of Canada, a government entity [17] to find the annual person-days not worked. We paired this with employment information from Statista [45] to generate the average days not worked due to industrial action per 1000 employees from 2011 to 2018. 2010 data was not available so the average was generated from 8 years instead of the 9 used for Europe. Australia’s data was gathered from a government-funded paper from the Australia Centre for Future Work [44]. The paper had exact data for the average days not worked due to industrial action per 1000 employees from 2010 to 2017 so no calculations were necessary. 2018 data were not available so the average was generated from 8 years instead of the 9 used for Europe.

Domestic data were taken from US Work Stoppages data provided by the US Bureau of Labor Statistics [48]. These data provide annual data and analysis of major work stoppages involving 1000 or more employees lasting one full shift or longer. We added up the work days idle by state by year from 2010 to 2018. If there were multiple states involved in a strike, we divided the number of workdays idle



equally for simplicity. We then compiled the state annual employment rates from the US Bureau of Labor Statistics. We paired the employment rates with the annual days idle by the state to calculate the average annual days not worked due to industrial action per 1000 employees. This calculation can be seen as follows:

Equation 1 Average days not worked

$$\begin{aligned} & \text{Average Days not worked due to work stoppage per 1000 employees} \\ &= \left( \sum_{i=2010}^{2018} \frac{\text{Total Days Idle in State in year } i}{\text{Total People Employed in State in year } i} \right) \div 9 \end{aligned} \tag{1}$$

In addition to work stoppages, the experts found during the DELPHI study that information concerning “right-to-work” laws was also an important factor in US Labor disputes, especially since many of these laws have been enacted in the last decade. Right-to-work laws are based on the general principle that employees should have the right to choose to join a union, but should not be forced to join a union as a stipulation of acquiring or maintaining employment [32]. Such legislation has been enacted in 27 states. When work stoppages or strikes occur in right-to-work states, there are likely non-union employees and/or temporary employees working allowing for continuous operation. This lessens the impact of a work stoppage on a plant in that state. Therefore, it is used in our methodology as a component of labor dispute.

## 11 Foreign Influence

The authors define foreign influence as factors that are country-dependent and influence US government supply chains. Not many studies discuss foreign influence as a risk since most studies were done in a single country [23] or the scope was not discussed [54]. Pettit [36] vaguely covers factors that could be perceived as foreign influence such as “political/regulatory change” within the category of “external pressures” but does not go into great detail. We chose to introduce foreign influence as a key factor within supply chain risk. This risk factor may play an even more important role in the future as many companies and governments may choose to move supply chains more regionally due to COVID-19. The three components that make up foreign influence in this study include foreign entity, human rights laws, and conflict minerals. Foreign entities are simply plants that are not located in the USA. There is always some degree of risk when a plant is not located within the country of the purchaser due to laws, regulations, and physical distance.

Human rights, as defined by the United Nations, are rights that are “inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and

education, and many more” [50]. They are important to supply chains because the USA has and can ban government contracts with countries that do not adhere to human rights laws. These violations can happen at any time and countries can get blacklisted without warning. One of the experts in the DELPHI study recalled prior experiences where the ban of a country caused supply chain disruption during an interview. To capture this factor, we use the Fragile States Index powered by the Fund for Peace. The index indicates countries where human rights were violated or unevenly protected. This includes pressures and measures related to press freedom, civil liberties, political freedoms, human trafficking, political prisoners, incarceration, religious persecution, torture, and executions [18].

Conflict minerals are generally defined as minerals mined in an area of armed conflict and traded illicitly to finance the fighting. The USA has legislation on four specific minerals, tantalum, tin, gold, and tungsten. For these minerals, companies must conduct a reasonable country of origin inquiry. If companies cannot prove the source of the minerals was not from a covered country (i.e., Angola, Burundi, Central African Republic, Republic of Congo, Rwanda, South Sudan, Tanzania, Uganda, and Zambia), they must submit a conflict minerals report. It is not illegal to source from the covered countries, but there is a lot of costly compliance that is required if sourced from a non-conflict-free country [39]. Therefore, as noted by several of the experts in the DELPHI study, the US government largely refrains from conflict mineral countries for any supplies, which makes plants in these countries a large supply chain risk.

## 12 DoD Dependence

Department of Defense (DoD) dependence refers to the proportion of defense/government spending vs the total global sales for a firm. If a company has a high dependence on DoD contracts, its plants are susceptible to DoD funding decisions. If a firm has low dependence on government contracts, the DoD is susceptible to the firm’s business decisions [42]. A company with a mixed DoD and commercial sales makeup, where proportions are close to 50/50 are the most safe to government purchasers. Though this category is not pertinent to most non-government purchasers, there are parallel categories that can be considered. For example, Pettit [36] has a connectivity category, which is defined as “the degree of interdependence and reliance on outside entities,” which can be used in place of DoD dependence in non-government firms. DoD dependence percentages were first collected via public accounting documents submitted to the SEC as found on EDGAR, the SEC’s online search tool, and through public annual reports found on company websites. If a firm’s DoD dependence was not available publically, SMEs in government were consulted for best estimates.

### 13 Financial Risk

Financial risk is defined as a firm potential for bankruptcy. A supply chain's health largely depends on the financial health of its suppliers. In fact, every expert consulted in the DELPHI study listed financial risk as the most important component of supply chain risk. Supplier bankruptcy can lead to select plant shutdowns at a minimum and company shutdown at a maximum. Company bankruptcy prediction models are not new and have been studied for decades [6]. There are a plethora of models that can be used by purchasers to aid in supply chain risk analysis; however, their use is uncommon. For example, Zsidisin et al. conducted a case study where seven companies were asked how their companies assessed supplier risk. None of them used a financial model backed by literature in their supply chain risk analysis or even a self-created financial bankruptcy risk model [54]. Due to the abundance of models in literature and Bellovary's [6] call for future research to focus on the use and application of existing models rather than the creation of new models, we use Dickerson et al.'s [14] model seen below to calculate a classification score. This model has proven to outperform other well-known military bankruptcy models of Dagele and Pepper [12], Liao and Moses [31], Godfrey [20], and the most popular general bankruptcy models in the literature of Ohlson [33] and Altman [1] at 92% average accuracy within a defense centric sample. There are many sources where you can gather the necessary variables for use in the Dickerson et al. model, the most comprehensive platforms that provide the necessary financial and market information for public corporations are S&P Global Capital IQ, and Wharton Research Data Services (COMPUSTAT).

Equation 2 Financial bankruptcy model [14]

$$Y = 1.423053E^{-11} X_1 + 6.535611E^{-10} X_2 - 4.467937E^{-3} X_3 - 2.102952E^{-4} X_4 \quad (2)$$

$X_1$  = Current assets

$X_2$  = Net income

$X_3$  = Total liabilities /total assets

$X_4$  = Current liabilities /current assets

$Y$  = Classification score.

The classification value  $c$  is then compared to a threshold value  $t$  such that if  $c < t$  the company is classified as expected bankrupt (1) else if  $c > t$  the company is classified as expected non-bankrupt (0). A common threshold for  $t$  is 0 and can be used as an initial baseline. However, if you are in a slightly different industry or outside of the United States and data are available, a known sample can be used to build a customized threshold value.

**Final Average Rankings from Experts**

Turbulence		Deliberate Threat		Foreign Influence			Overall				
Natural Disasters	Geopolitical Disruptions	Terrorism	Labor Disputes	Human Rights Laws	Conflict Minerals	Foreign Entity	Turbulence	Deliberate Threat	Financial Risk	Foreign Dependence	DoD Dependence
57	43	41	59	26.5	23.5	50	10	12	35	21	22

**Exhibit 5** Final average rankings from experts

## 14 Risk Weights

The risk weights seen in Exhibit 5 were determined through the survey in Exhibit 1. Basic sensitivity analysis was done, and there was little change in accuracy with a + or – change of <5% on individual weights. However, with changes of >5% there were great losses in accuracy indicating that the weights are likely in the correct realm. To calculate initial overall risk ratings, the general formula is used within each risk criterion where *i* represents the component and *n* is the total number of components within that category. Note that the observational categories of these values could change with the heuristic.

Equation 3 Average risk calculation per category

$$\begin{aligned}
 & \text{Risk Category Overall Ranking} \\
 & = \left( \sum_{i=1}^n \text{rating}_i * \frac{\text{final average ranking from expert}_i}{100} \right) \div n \quad (3)
 \end{aligned}$$

## 15 Ratings

The data sources for each component varied in terms of scale; therefore, for each component, input data were standardized into a rating from 0 to 5. The cutoffs for these ratings were usually determined by the data source itself through severity breaks in map keys or language within the document. If such a framework for cutoffs was not present in the data source, it was determined by the authors. The table below shows the cutoffs for the different components and categories. A “[ indicates the number is included within the range whereas a’)” indicates the number is not included in the range. This can be seen in Exhibit 6.

	Natural Disasters USA	Natural Disasters Foreign	Geopolitical Disruptions	Terrorism	Right to Work USA	Work Stoppages	Financial	Human Rights	Conflict Minerals	Foreign Entity	DoD Dependence
5 (High Risk)	17+	(0,20]	<50	8+	Law not present	25	1 (Expected Bankrupt)	60+	countries listed in Section 1502 of the Dodd Frank Act	Foreign Country	85+ or ≤ 15
4	[15,17)	(20,30]	[50-60)	[6,8)	N/A	(15,25)	N/A	[50,60)	N/A	N/A	(15,20] or [80,85)
3 (Mid Risk)	[13,15)	(40,65]	[60,70)	[4,6)	N/A	(10,15)	N/A	[40,50)	N/A	N/A	(20,30] or [70,80)
2	[10,13)	(65,85]	[70,80)	[2,4)	N/A	(3,10)	N/A	[30,40)	N/A	N/A	(30,40] or [60,70)
1	(0,10)	85+	80+	(0,2)	N/A	(1,3)	N/A	(0,30)	N/A	N/A	(40,60)
0 (No Risk)	0	N/A	N/A	0	Law Present	0	0 (Expected Non-Bankrupt)	0	All other countries	USA	N/A

Exhibit 6 Data to score conversion chart

## 16 Assigning Risk Scores to Observational Categories

In traditional multicriteria scoring systems, the more components that are added to a category, the lesser the relative impact of a single risk component. Likewise, the more categories that are added to the risk component the amount of weight each category carries lessens. In these cases, the “risk indices are less sensitive to a large risk rating on any one factor . . . such that the riskiness of a supplier can become ‘lost’ in the morass of the factors measured” [7]. To mitigate this, we have created a heuristic such that high-risk individual components are not lost in the overall rating.

Initially, each plant will be assigned a numerical score in each category and an overall numerical score, which is the average of its category ratings that were assigned in Exhibit 6 resulting in a final score from 0 to 5. The category scores and final scores will be converted into observational categories of good, watch, or alert. A score from [0, 3.5) will be assigned good, [3.5, 4.5) watch, and [4.5, 5) alert. After the initial ratings are assigned to observational categories, we run the heuristic to identify any risky plants that may have become lost in the average score. To do this, we assign the same observational categories of good, watch, and alert to each of the components and categories.

The conversion cutoffs will vary by component as seen in Exhibit 7, as recommended by a SME with no rounding (IE a 3.75 will fall in the 3 row). The heuristic will upgrade the observational rating of a category or overall rating of a plant in the following circumstances (the heuristic will never downgrade an observational rating):

### Heuristic per Category

1. Every plant that has a component of a category of alert will upgrade the overall category to alert.
2. Every plant that has a component of watch will upgrade the overall category to watch.

### Heuristic Overall

1. Every plant that has an alert in any category will automatically be upgraded to watch.

Data to Rating Conversion Chart

	Natural Disasters USA	Natural Disasters Foreign	Geopolitical Disruptions	Terrorism	Labor Disputes	Financial	Human Rights	Conflict Minerals	Foreign Entity	DoD Dependence
5 (High Risk)	Alert	Alert	Alert	Alert	Alert	Alert	Alert	Alert	Alert	Alert
4	Watch	Watch	Alert	Watch	Watch	N/A	Alert	N/A	N/A	Watch
3 (Mid Risk)	Good	Good	Watch	Good	Good	N/A	Watch	N/A	N/A	Good
2	Good	Good	Good	Good	Good	N/A	Good	N/A	N/A	Good
1	Good	Good	Good	Good	Good	N/A	Good	N/A	N/A	Good
0 (No Risk)	Good	N/A	N/A	Good	Good	Good	Good	Good	Good	N/A

Exhibit 7 Score to rating conversion chart

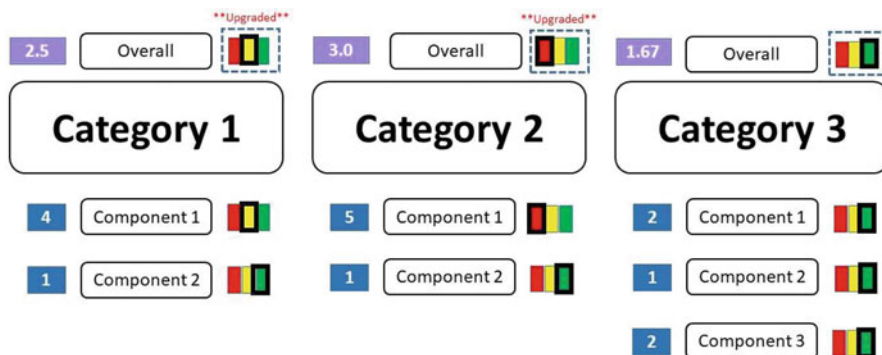
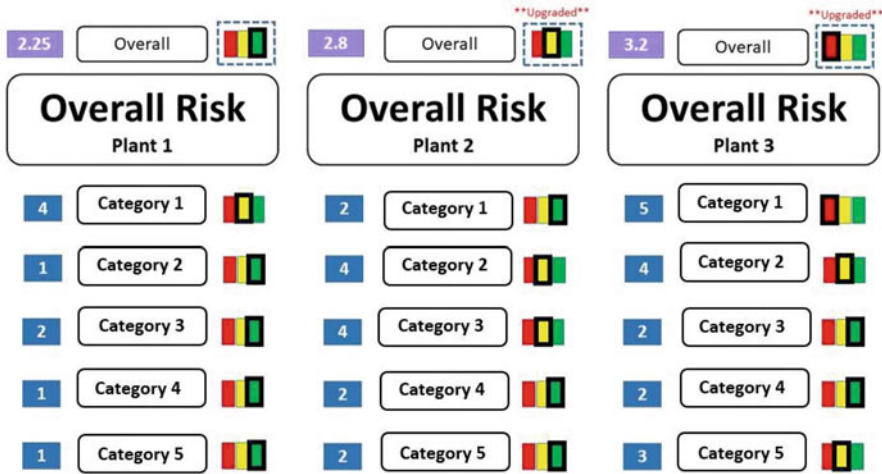


Exhibit 8 Category observation ratings

- Any plant that has watch in two or more categories will be upgraded to watch.
- Any plant that has alert in two or more categories will be automatically upgraded to alert.
- Any plant that has at least one alert, and two or more watches will automatically be upgraded to alert.

Exhibit 8 depicts how this heuristic would work in terms of category observational ratings. The red, yellow, and green colored tiles represent the observational categories of alert, good, and watch, respectively. Category 1 gets upgraded from good to watch due to rule #2 of the category heuristic. Category 2 gets upgraded from good to alert due to rule #1 of the heuristic. Category 3 is unaffected by the heuristic and its original rating stands.

Exhibit 9 shows how this heuristic can influence overall observational ratings. The tiles represent the same categories as in Exhibit 8. Here, Plant 1 is unchanged by the heuristic. Plant 2 is upgraded from good to watch due to rule #2 of the heuristic. Lastly, Plant 3 is upgraded from good to alert in Plant 3 due to rule #4 of the heuristic. In these examples, one can see that averages can often hide risky



**Exhibit 9** Overall observational ratings

firms. This is especially present in Plant #3, which is very risky, but its overall initial numerical score of 3.2 put it into the good category.

## 17 Results

**Sample Company Testing** In order to test the efficacy of the model, we used two different data sets from US government supplier plants. One data set consisted of data gathered prior to the COVID-19 pandemic, which we classify as “non-crisis” data. This sample includes 26 supplier firms and their 381 domestic plants and 34 foreign plants. According to Theiler [46], classification problems with a matched-pair structure have significantly better classification accuracy so we build the data such that there are an equal number of plants that have closed and not closed in the data set. From this sample, we built a matched-pair subsample, which consisted of 22 closed plants and 22, which are still active. The 22 that have closed were identified via government data and the 22 which are still active were selected randomly from the 393 remaining plants from the original sample. The sample size is limited by the number of plant closures in a year, which generally ranges from 5% to 10%. In order to maintain a matched-pair sample, we were limited by the 22 closures in pre-COVID-19 sample data. Exhibit 10 shows the results where the model proves to be 95.5% accurate in non-crisis situations. Since over 50% of plants were classified as “good,” this reduces the number of plants to be further examined by over 50% saving numerous analyst hours.

**Exhibit 10** Non-crisis accuracy

	Initial Testing
Accuracy	95.5%
False Positive	0% (Alert) 13.6% (Watch)
False Negative	4.5% (Good)

**Exhibit 11** Crisis (COVID-19) accuracy

	Initial Testing
Accuracy	93.8%
False Positive	0% (Alert) 16.7% (Watch)
False Negative	6.2% (Good)

The secondary sample consisted of US government supplier plant closures that occurred during the COVID-19 Pandemic. As one would expect, there were a larger amount of closures during this crisis time. We were able to build a sample of 48 closed plants and 48 active plants. Again, the sample size is limited by the number of closed plants to build the matched-pair sample. The 48 active plants were randomly selected from a sample of 52 firms consisting of 277 domestic plants and six foreign plants. Exhibit 11 shows the results where the model proves to be 93.8% accurate in crisis situations. In this case, over 40% of plants were classified as “Good” and this reduces the number of plants to be further examined by over 40% saving numerous analyst hours.

Based on these samples and results, we see that the hybrid supplier risk assessment model performs well in both crisis and non-crisis environments. The model performs slightly better in non-crisis situations but not significantly. It is important to note that both results have low false-negative values. This is important as false negatives indicate that a plant closed without prior prediction. Alternatively, false positives of “watch” simply mean an analyst must look at these companies in further detail. Upon further examination, it is unlikely that the plants would be falsely classified by an analyst.

## 18 Conclusion

We have built a novel multicriteria scoring model for purchasing agents within the defense industry. Through the use of the DELPHI method using expert input to determine risk weights, we have answered the call proposed by Blackhurst for “practical methods for determining risk weights need to be evaluated and examined” [7]. We have also identified several public data sources that can feed into different risk factors and created an appropriate standardized rating system for such data. Lastly, we have created a heuristic that prevents large component risk factors from slipping through the cracks in a multicriteria model based on average values. We also show that the model can be successful in both situations of crisis and non-



crisis. We acknowledge that this case study was done on a relatively small sample size and hope that this model can be applied on larger data sets.

**Further Applications** While we have shown the use of our model for a government purchasing agent, the use of risk models should not be limited to public agencies. Private firms should also demonstrate concern for their suppliers' health [2]. Financial information for private firms is notably harder to attain and most financial models only utilize public data [1, 14, 33]. However, this model could be modified to capture the financial information of private companies in a different way. This model can also be applied to different industries such as auto-manufacturing, computer manufacturing, and even restaurant food purchasers.

**Acknowledgements** The author thanks the cadets who helped shape the financial model used in this paper, Isaac J. Antony, Rodrigo R. Artolozaga, Mary E. Bell, Brett R. Boswell, William D. Dickerson, Joshua N. Kim, Benjamin T. Berry, Angel J. Espinoza, and Alexander P. Sobeski. The author acknowledges the assistance provided by several US government organizations in data collection. The author also thanks the co-organizers of the 2022 INFORMS Business Analytics Conference and attendees for providing feedback and anonymous reviewers for helpful suggestions on an earlier version of this paper.

## References

1. Altman, E.I.: Discriminant analysis and the prediction of corporate bankruptcy. *J. Financ.* **23**(4), 589–609 (1968)
2. Altman, E., Hotchkiss, E.: *Corporate Financial Distress and Bankruptcy: Predict and Avoid Bankruptcy, Analyze and Invest in Distressed Debt*, 3rd edn. Wiley, New York (2005). <https://doi.org/10.1002/9781118267806>
3. Baryannis, G., Dani, S., Antoniou, G.: Predicting supply chain risks using machine learning: the trade-off between performance and interpretability. *Futur. Gener. Comput. Syst.* **101**, 993–1004 (2019a). <https://doi.org/10.1016/j.future.2019.07.059>
4. Baryannis, G., Validi, S., Dani, S., Antoniou, G.: Supply chain risk management and artificial intelligence: state of the art and future research directions. *Int. J. Prod. Res.* **57**(7), 2179–2202 (2019b). <https://doi.org/10.1080/00207543.2018.1530476>
5. Beaver, W.H.: Financial ratios as predictors of failure. *J. Account. Res.* **4**, 77–111 (1966)
6. Bellovary, J.L., Giacominio, D.E., Akers, M.D.: A review of bankruptcy prediction studies: 1930 to present. *J. Financ. Educ.* **33**, 1–42 (2007)
7. Blackhurst, J.V., Scheibe, K.P., Johnson, D.J.: Supplier risk assessment and monitoring for the automotive industry. *Int. J. Phys. Distrib. Logist. Manag.* **38**, 143–165 (2008)
8. Bower, A.G., Garber, S.: *Statistical Forecasting of Bankruptcy of Defense Contractors: Problems and Prospects*. RAND – Project Air force (1994)
9. Cambell, J., Hilscher, J., Szilagyi, J.: In search of distress risk. *J. Financ.* **63**, 2899–2939 (2008)
10. Columbia University: US Natural Hazards Index. National Center for Disaster Preparedness, Earth Institute (2020)
11. Cranfield University: *Supply Chain Vulnerability: Executive Report*. School of Management (2002)
12. Dagel, H.W., Pepper, R.M.: A financial distress model for DoD hardware contractors. *J. Parametrics.* **10**(1), 5–40 (1990). <https://doi.org/10.1080/10157891.1990.10462471>

13. Dalkey, N., Helmer, O.: An experimental application of the DELPHI method to the use of experts. *Manag. Sci.* **9**(3), 458–467 (1963). <https://doi.org/10.1287/mnsc.9.3.458>
14. Dickerson, D., Boswell, B., Sobeski, A., Antony, I., Artolozaga, R., Sanders, I.: Forecasting bankruptcy within department of defense suppliers using linear discriminant analysis. In: Proceedings of the Annual General Donald R. Keith Memorial Conference (2022).
15. Eberle, A.O.: Risikomanagement in der Beschaffungslogistik – Gestaltungs-empfehlungen für ein System, dissertation. University of Bamberg, Bamberg (2005)
16. Eckstein, D., Kunzel, V., Shafer, L., Wings, M.: Global Climate Risk Index 2020: Who Suffers the Most from Extreme Weather Events? Weather-Related Loss Events in 2018 & 1999–2018. Germanwatch (2020)
17. Employment and Social Development Canada: Work Stoppages by Jurisdiction and Year. Government of Canada. Date Accessed 04 August 2020. \*Referred to in paper as ESDC (2020)
18. Fund for Peace: Fragile States Index Annual Report 2019. Fragile States Index. Fund for Peace. \*Referred to in paper as FFP (2019)
19. General Litigation Branch: Contracting Officer’s Guide to Bankruptcy, Army Litigation Division (2012)
20. Godfrey, I.C.: Predicting Bankruptcy in the Air Force. (Master’s thesis). Air Force Institute of Technology (1990)
21. Green, K., Armstrong, J., & Graefe, A. Methods to elicit forecasts from groups: Delphi and prediction markets compared. *Foresight: The International Journal of Applied Forecasting* (2007)
22. Institute for Economics & Peace: Global Terrorism Index 2019: Measuring the Impact of Terrorism, Sydney, November 2019. Available from: <http://visionofhumanity.org/reports> (accessed 01 June 2020). \*referred to in the paper as IFEP (2019)
23. Jung, K., Lim, Y., Oh, J.: A model for measuring supplier risk: do operational capability indicators enhance the prediction accuracy of supplier risk? *Br. J. Manag.* **22**, 609–627 (2011)
24. Kersten, W., Boger, M., Hohrath, P., Spath, H.: Supply chain risk management: development of a theoretical and empirical framework. In: Kersten, W., Blecker, T. (eds.) *Managing Risks in Supply Chains*. Springer (2006)
25. MacCarthy, B.L., Atthirawong, W.: Factors affecting location decision in international operations – a Delphi study. *Int. J. Oper. Prod. Manag.* **23**(7), 794–818 (2003)
26. Marsh: Political Risk Map 2020: Trade Tensions Threaten Political Stability. Marsh JLT Specialty, Marsh (2020)
27. Mason, R.: Coping with complexity and turbulence – an entrepreneurial solution. *J. Enterprising Cult.* **14**(4), 241–266 (2006)
28. Mason-Jones, R., Towill, D.R.: Shrinking the supply chain uncertainty cycle. In: Control, pp. 17–22. Logistics Systems Dynamics Group, Cardiff (1998)
29. Matook, S., Lasch, R., Tamaschke, R.: Supplier development with benchmarking as part of a comprehensive supplier risk management framework. *Int. J. Oper. Prod. Manag.* **29** (2009)
30. MH&L Staff: Supply Chain Experiencing High Rate of Terrorist Attacks. Material Handling and Logistics. Global Supply Chain (2017)
31. Moses, D., Liao, S.: On developing models for failure prediction. *J. Commercial Bank Lending.* **69**, 27–38 (1987)
32. National Right to Work Committee.: Message form the National Right to Work Committee Chairman (2020)
33. Ohlson, J.A.: Financial ratios and the probabilistic prediction of bankruptcy. *J. Account. Res.* **18**(1), 109–131 (1980)
34. Organization of American States, Department of Regional Development; Natural Hazards Project; United States Agency for International Development, Office of Foreign Disaster Assistance: Disaster, planning and development: managing natural hazards to reduce loss (PDF). Organization of American States. Washington DC (1990)
35. Peck, H., Christopher, M.: The Five Principles of Supply Chain Resilience. *Logistics Europe*, February (2004)

36. Pettit, T., Fiksel, J., Croxton, K.: Ensuring supply chain resilience: development of a conceptual framework. *J. Bus. Logist.* **34**, 1–21 (2010)
37. Pettit, T., Croxton, K., Fiksel, J.: Ensuring supply chain resilience: development and implementation of an assessment tool. *J. Bus. Logist.* **34**, 46–76 (2013)
38. Rice, J.B.: Prepare Your Supply Chain for Coronavirus. *Harvard Business Review*. Harvard University. (2020)
39. SEC (2017) Fact sheet: disclosing the use of conflict minerals. U.S. Securities and Exchange Commission. <https://www.sec.gov/opa/Article/2012-2012-163htm%2D%2D-related-materials.html>. Accessed 5 Aug 2020
40. Shumway, T.: Forecasting bankruptcy more accurately: a simple hazard model. *J. Bus.* **74**, 101–124 (2001)
41. Sinha, P., Whitman, L.E., Malzahn, D.: Methodology to mitigate supplier risk in an aerospace supply chain. *Supply Chain Manag. Int. J.* (2004). <https://doi.org/10.1108/13598540410527051>
42. Sleeper, S., Starns, J., Warner, E.: Identifying and mitigating industrial base risk for the DoD: results of a pilot study. In: AFCEA Acquisition Research Symposium (2014)
43. Sodhi, M.S., Son, B.-G., Tang, C.S.: Researchers' perspectives on supply chain risk management. *Prod. Oper. Manag.* **21**(1), 1–13 (2012). <https://doi.org/10.1111/j.1937-5956.2011.01251.x>
44. Stanford, J.: Briefing Note: Historical Data on the Decline in Australian Industrial Disputes, p. 3. The Australia Institute, Centre for Future Work (2018)
45. Statista: Unemployment Canada <https://www.statista.com/statistics/578362/unemployment-rate-canada/>, <https://www.statista.com/statistics/464156/number-of-full-time-workers-in-canada/> (2020)
46. Theiler, J.: Matched-pair machine learning. *Technometrics.* **55**(4), 536–547 (2013). <https://doi.org/10.1080/00401706.2013.838191>
47. Tinoco, M.H., Wilson, N.: Financial distress and bankruptcy prediction among listed companies using accounting, market and macroeconomic variables. *Int. Rev. Financ. Anal.* **20** (2013). <https://doi.org/10.1016/j.irfa.2013.02.013>
48. U.S. Bureau of Labor Statistics: U.S. Work Stoppages. U.S. Bureau of Labor Statistics. Retrieved 20 July 2020. \*Referred to as USBLS in paper (2020)
49. U.S. Courts: Caseload Statistics Data Tables. Table F-2: U.S. Bankruptcy Courts—Business and Nonbusiness Cases Filed, by Chapter of the Bankruptcy Code—During the 12-Month Period Ending March 31, 2019. U. S. Courts. Administrative Office of the U.S. Courts. Retrieved 20 July 2020 (2019)
50. United Nations: Human Rights. Global Issues. United Nations (2020). <https://www.un.org/en/sections/issues-depth/human-rights/>. Accessed 14 Aug 2020
51. Vandaele, K.: Strikes' Map of Europe. European Trade Union Institute (2019). Retrieved 20 July 2020
52. Wentholt, M.T.A., Rowe, G., Konig, A., Marvin, H.J.P., Frewer, L.J.: The views of key stakeholders on an evolving food risk governance framework: results from a Delphi study. *Food Policy.* **34**, 539–548 (2009)
53. Zsidisin, G.A.: Managerial perceptions of supply risk. *J. Supply Chain Manag.*, 14–26 (2003). <https://doi.org/10.1111/j.1745-493X.2003.tb00146.x>
54. Zsidisin, G.A., Ellram, L.M., Carter, J.R., Cavinato, J.L.: An analysis of supply risk assessment techniques. *Int. J. Phys. Distrib. Logist. Manag.* **34**(5), 397–414 (2004)

# Quantum Computers: The Need for a New Cryptographic Strategy



Britta Hale, Nina Bindel, and Douglas L. Van Bossuyt

## 1 Introduction

“Quantum computing” is a term filled with both enigma and possibility—but one with very concrete potential effects on the security and stability of daily life. The word “quantum” refers to the smallest possible unit of quantity, and finessing our current computation approaches to achieve even finer-grained control is certainly an intriguing possibility. Thus, it is no surprise that quantum computing is an area of research and development attracting both investors and startups [36, 58, 90, 98]. For all systems, including industrial control systems (ICS), government systems, and defense systems, quantum computing offers not only opportunity but also risk. One of the capabilities that a quantum computer presents includes breaking of certain cryptographic primitives in their current form [61]. Cryptography—the backbone of security infrastructures around the world—propels even the slightest risk into magnified focus [92, 101]. In this chapter, we provide an overview of the risk of quantum computing to security and considerations to weigh in system hardening for quantum resistance, with tailoring to a strategic management and governance audience. Specifically, we provide context that decision-makers and engineers can use in preparing for the coming quantum threat with consideration to the amount of time needed to update existing fielded systems to meet the threat, as well as systems still to be developed.

---

B. Hale (✉) · D. L. Van Bossuyt  
Naval Postgraduate School, Monterey, CA, USA  
e-mail: [britta.hale@nps.edu](mailto:britta.hale@nps.edu); [douglas.vanbossuyt@nps.edu](mailto:douglas.vanbossuyt@nps.edu)

N. Bindel  
SandboxAQ, Palo Alto, CA, USA  
e-mail: [nina.bindel@sandboxaq.com](mailto:nina.bindel@sandboxaq.com)

In the remainder of this section, we provide high-level background information on cryptography and quantum computing to set the stage for the remainder of the chapter. We further outline the rest of the chapter at the end of this section.

## 1.1 *Cryptography*

Cryptography is a science and art based on extrapolating a little secret information to build larger architectures of security. For example, encryption offers the property of confidentiality, under which an attacker is unable to read data; it provides confidentiality through use of a small amount of secret information, that is, an encryption key. Only parties privy to the decryption key can access the data. Confidentiality is an important security goal when, for example, data is stored or communicated across networks [106]. Other important security properties offered by cryptography include authenticity and integrity. Algorithms providing authenticity and integrity, for example, *message authentication codes* and *digital signatures*, ensure that only parties with access to a secret key (authenticity) can modify the data (integrity), thus preventing forgeries and data manipulation [57].

Cryptography can be further divided into symmetric techniques (where a sender and receiver both have a copy of the same secret key) and asymmetric techniques (where only one party has the secret decryption key and all other parties have access to a *public* encryption key). Asymmetric encryption, also called public key encryption, allows anyone to send an encrypted message while only the holder of the secret key can decrypt, much like a drop-box. In contrast, for symmetric encryption, both parties use the same secret key for encryption and decryption. Usually symmetric encryption is used to store data, while for data in transit a mix of both—symmetric and asymmetric techniques—is used. More specifically, asymmetric techniques are used to exchange/agree on the secret key, which is then used to encrypt the data using symmetric techniques.

Asymmetric authentication can be achieved through digital signatures, with which one party signs data using a secret signing key (known only to the signer) while anyone (using a public verification key) can verify the signature. Likewise, there are corresponding symmetric techniques for when both parties possess a secret authentication key [97]. There is any entire field of research on cryptographic techniques and properties [62]; the above context suffices as a high-level introduction for the reader to this chapter.

## 1.2 *Quantum Computers*

Compared to our current transistor-based computers that compute over bits with state 0 or 1, quantum computers use the principles of quantum physics for computations. More concretely, this new generation of computers saves, processes,

and communicates data in the form of quantum states, also called qubits. While small quantum computers can already be built, such as Google's 72-qubit quantum computer [54], this technology is still in its infancy. To be of serious risk, for example, to break certain instances of deployed cryptographic algorithms, several million qubits are necessary [37]. While the difference between 72 and several million qubits seems huge, quantum computing experts estimate that quantum computers large enough to break certain currently used cryptographic algorithms will be built within the next 14 to 30 years [65]. However, as stated by the National Institute for Standard and Technology (NIST) [19], "Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing." Consequently, we take a closer look at system security implications of a quantum computer, the urgency of system transition, and key considerations for preparing for the transition to quantum resistance in complex systems.

### ***1.3 When Systems Rely on Broken Cryptography***

The importance of ensuring systems are operating with modern cryptography can be illustrated by issues with video feed hacks of uncrewed aerial systems (UASs). At least one incident of a UAS video feed being hacked is recorded in the open literature where an adversary was able to use the hacked video feed to injure or kill defense forces [56]. In such situations even if a UAS is only providing intelligence, surveillance, and reconnaissance (ISR), and has no weapons aboard, the ISR information can be damaging to national security and with potentially deadly outcomes. Thus, while it may be tempting to use old UAS systems especially in times of crisis, it is important to ensure cryptography is current so that unintended consequences do not occur. Further, any system that contains digital information should be protected to ensure the data is safe today and in the future. The following sections will investigate what this means for systems in the context of a quantum attack, extending the illustrated context of a classic attack on cryptography.

### ***1.4 Outline***

This chapter discusses how the threat of quantum computing impacts security for current systems and what considerations should be taken into account when preparing for it. As such, we start with explaining what the quantum threat is in Sect. 2. More concretely, we explain the implications for single cryptographic building blocks as well as the security of entire systems. In addition, we also touch upon legal and economic implications.

Moving on, Sect. 3 presents ways to prepare for the quantum threat. This includes explaining different approaches that exist (i.e., using “post-quantum” or “quantum” cryptography) and their differences. From that subsection on, this chapter concentrates on “post-quantum” cryptography and the “post-quantum” transition, with reasoning provided. Since a post-quantum transition might come with significant efforts and delaying the transition might pose severe security risks—both depending on the particular system—it is important to analyze preparation timeline. Tools for this analysis are explained in Sect. 3.2.

Moving forward, Sect. 4 takes a closer look at the range of factors to model and consider for systems when looking to integrate post-quantum solutions. We also cover common industry approaches to post-quantum cryptography and fallacy risks to avoid. Section 5 provides an overview of various critical and major system operations, what types of risks quantum computing may pose for such systems, and presents a risk modeling perspective.

## **2 The Quantum Threat and Its Implications**

Quantum computers have frequently been juxtaposed with cryptography as a threat to currently deployed systems. One reason is that quantum computers have the potential to break most of the currently deployed asymmetric cryptography; however, they do not have the same devastating effect on the security of symmetric cryptography. In this section, we take a closer look at the cryptographic and broader security implications of a quantum computer, also called the “quantum threat.” In particular, we first explain the implications of cryptographic algorithms using examples. We then explain how broken security guarantees of cryptographic building blocks affect the security of systems. We end this section by touching upon the legal and economic implications of the quantum threat.

### ***2.1 Implications for Cryptography***

This section explains why and how large quantum computers can break most of our currently deployed asymmetric cryptography.

As described above, for asymmetric encryption, everyone who knows the public encryption key can encrypt a message but only holders of the secret decryption key can decrypt ciphertexts (other asymmetric cryptographic algorithms work in analogous ways). That means for the encryption scheme to be secure it must not be possible to compute the secret key from the public key—yet for decryption to be possible at all, the two keys must be related. In particular, it must be easy to compute the public key from the secret key but practically impossible to compute the secret

from the public key. This can be realized using *computationally hard mathematical problems*. For example, the *integer prime factorization problem* says that given two large prime numbers it is easy to multiply them; however, given such a large product, it is *computationally hard* to compute the prime factors.

One of the most famous asymmetric encryption schemes—the RSA scheme invented by Rivest, Shamir, and Adleman [91]—is based on this construction principle. The public key is the product of two prime numbers, while the secret key is some information that enables finding the prime factors. For further details on modern cryptography, see Katz and Lindell [53]. As far as we know, no classical algorithm (i.e., algorithms run on our current transistor-based computers) solves the prime factorization problem efficiently (i.e., in polynomial time) that would allow breaking of RSA [68]. However, there exists an algorithm—Shor’s quantum algorithm [95]—that solves this computational problem efficiently when running on a sufficiently large quantum computer.

Another very important computational problem that is currently a security basis for most deployed cryptographic systems is the *discrete logarithm problem* [51]. We omit the details here as for the following discussion it is sufficient to know that this problem can also be solved efficiently using Shor’s quantum algorithm. We call a quantum computer *cryptographically relevant* if it is able to break instances of currently deployed cryptographic algorithms, such as RSA-2048, in a reasonable time (where “reasonable” is contingent on the application).

Interestingly, Shor’s algorithm does not seem to give a computational advantage in breaking symmetric cryptographic algorithms. While another quantum algorithm, namely Grover’s quantum algorithm [38], does provide a slight speed-up for attacks, it can be mitigated by essentially doubling the key length. For more details, we refer to [10].

In a surface-level assessment, this observation could be interpreted to imply that quantum resistance is realizable by simply foregoing asymmetric cryptographic techniques in favor of symmetric cryptographic algorithms throughout a system. However, as we will discuss in Sec. 4.1, such an approach is naive and introduces a multitude of risks that current systems have been made robust against. Many of those risks would be immediate—exploitable by standard adversaries without need for a quantum computer. We will discuss countermeasures in Sect. 3.1, but first take a look at the broader system security implications of the quantum threat as second- and third-order effects from breaking cryptographic algorithms.

To further compound the above risks, there is an additional approach termed *back-tracking attacks* that further magnifies the effects of an eventual attack. The back-tracking attack scenario is already taking place now—*before* large quantum computers exist. Under this attack, encrypted and authenticated communication information is captured and collected. Huge amounts of such encrypted data are then stored. Once a suitable quantum computer is available, the attacker can decrypt the stored ciphertext and the collected data becomes available and actionable to the attacker.

Notably, this approach has an added benefit to the adversary, namely through data aggregation. The concept of *classification by compilation* is common for



sensitive information [17, 50], and applies to the increased risk of disclosing sensitive information when an adversary is able to associate various data pieces and make deductions from them. Naturally, back-tracking attacks motivate transition to quantum-resistant cryptography far earlier than a quantum computer is actionable. The more data that is communicated as quantum-resistant ciphertexts, the more data stays confidential also in the future.

Moving forward, the next subsection describes how breaking the security of cryptographic algorithms impacts the guarantees of security systems.

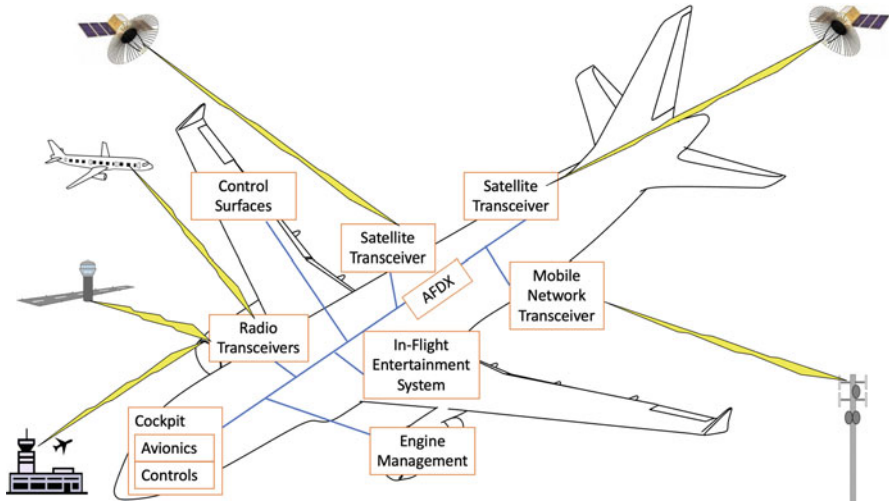
## 2.2 *Implications for Security*

Merging from core cryptographic security into system security leads us to a wider view of integral parts and dependencies—as well as security risks and implications. System security relies on principles from the C-I-A triad, that is, confidentiality–integrity–authenticity. These system goals are applied to different system components, with varying degrees of requirements. For example, data confidentiality is essential if an adversary could collect or utilize information and authenticity ensures protections against impersonation of components. Tying together integrity and authenticity, we have that data received from a given component is authentic to the source, which avoids malicious injections.

Cryptography forms the foundation for the security of these systems as a whole. While there are numerous security measures that a system can take, those become largely irrelevant if the foundation crumbles. Under a cryptographically relevant quantum computer, the current security C-I-A guarantees no longer hold [10]. Such quantum attacks could have devastating implications for the wider system at the time of attack and thereafter. For example, consider the case of a crewed aircraft where a quantum computer is existent (a more detailed discussion on system security implications and back-tracking attacks for such cases will be covered in Sect. 5).

Figure 1 illustrates a concept of operations (CONOPS) of the aircraft from the perspective of the variety of communications links acting on the system and connecting the wider system of systems (SoS).

Failure of C-I-A security guarantees has numerous consequences in the crewed aircraft SoS. For example, among external communication links, aircraft depend on satellite systems for navigation. Attacks in real time could potentially lead to mid-air collisions or other adverse effects (back-tracking attacks could also lead to traceability for past sensitive defense missions, or forgeability of past location data to subvert auditability). Compromise of individual communication links and associated type(s) of C-I-A security have differing effects on the SoS, ranging from undesirable loss of sensitive information to catastrophic loss of the aircraft itself.



**Fig. 1** Crewed aircraft internal systems. A modern crewed aircraft contains many interconnected systems that operate on internal networks such as Avionics Full-Duplex Switched Ethernet (AFDX). Several systems that may be connected to AFDX or similar networks are shown. External communications with satellites, other aircraft, and the ground are shown. Additionally, crew and passengers interact with the AFDX or similar network through avionics, control systems, and the in-flight entertainment system

### 2.3 *Legal and Economic Implications*

Security implications of a quantum computer extend past the technological threat and into the social, economic, and legal spheres. Research has analyzed how allies such as the United States, the European Union (EU), the United Kingdom, Australia, Canada, and New Zealand attempt to govern the quantum threat by studying diverse public documents, as well as how the quantum threat is perceived by the different actors [22]. Csenkey and Bindel [22] found that many public documents describe the threat as a technical threat and mention the back-tracking attack as described above. Interestingly, however, they also observed that the quantum threat is perceived as a legal issue. For example, the EU's regulatory requirements for data privacy and security might be violated by quantum attacks, creating both legal and socioeconomic implications.

In addition, it has also been found that the quantum issue is perceived as an economic threat [22] due to breaks in security, with particular risk to supply chains or business continuity. Implications from this are twofold: businesses must adapt and account for the post-quantum transition, and they may elect or be forced to shorten supply chains or find new suppliers to meet regulations if existing supply chain partners have not (yet) transitioned to post-quantum secure alternatives. This is particularly important in complex systems such as the above-described ecosystem surrounding crewed aircraft.

While this chapter concentrates on the technical and system-level issues for a post-quantum transition, it should not be forgotten that the security reasons for undertaking such a transition have repercussions at various levels of society. Cybersecurity underpins much of the digital and larger cyber-domain today, and even seemingly unrelated operations with any fringe connection using software, hardware, the Internet, or radio frequency transmissions are liable to be impacted. Thus, the impact of disregarding the quantum threat goes well beyond technical implications and might threaten almost all aspects of our daily lives, economy, and society.

To conclude this section, quantum computing presents a risk to asymmetric cryptography—a core foundation to many systems today. Thus, by implication, quantum computing poses a significant risk to wider systems. Such security risks have third-order effects on auditability, civil rights, and even supply chain integrity, leading to an urgency for action in support of legal and economic functions that may be seemingly far removed from cybersecurity considerations. In the next section, we will take a closer look at cryptographic tools and preparation timelines.

### 3 Preparing for the Quantum Threat

Inventing (or even standardizing) alternative quantum-secure cryptography is just the first of many steps required to prepare for the quantum threat. Consequently, in this section, we look at not only basic quantum resistant cryptographic solutions but other factors and timeline implications of a transition to post-quantum cryptography.

#### 3.1 *Post-Quantum Cryptography vs. Quantum Cryptography*

Currently, there are two main cryptographic directions that use the term “quantum”: post-quantum cryptography and quantum cryptography. Naturally such similarity in terms can lead to confusion, with potential consequences in procurement of system solutions that may not solve the intended security problem.

The first approach, quantum resistant or *post-quantum (PQ)* cryptography, is designed for the explicit goal of defense from a quantum adversary.<sup>1</sup> Collectively, such techniques are called *post-quantum cryptography (PQC)*, and in particular algorithms are called, for example, post-quantum digital signatures, post-quantum public-key encryption algorithms, etc. Researchers, industry, and standardization bodies have been working on post-quantum secure alternatives for more than 15

---

<sup>1</sup> Early schemes such as the code-based McEliece and the lattice-based NTRU encryption scheme that have been designed in the 1970s and 1990s, respectively, have not explicitly been designed to resist quantum adversaries.

years. In 2017, NIST started standardization of post-quantum public-key encryption and digital signature algorithms [2].

This approach enables use of current public-key infrastructure and relies on switching out the cryptographic algorithms being used. In a more concrete example, a quantum-vulnerable algorithm like RSA must be substituted with post-quantum algorithms. Post-quantum algorithms are based on different mathematical construction principles that are not known to be efficiently solvable by quantum algorithms. Post-quantum secure algorithms are constructed over different computationally hard problems than quantum-vulnerable algorithms. Thus, new algorithms are not vulnerable to Shor’s quantum algorithm. Much research has been done on the selected computationally hard problems [9, 33, 76] as new alternatives to the prior selections.

Notably, post-quantum cryptography is designed to be run on current transistor-based computers. Hence, no physical changes have to be made to the infrastructure. It does not require any special (i.e., quantum) equipment to protect against the threat. However, post-quantum algorithms do come with different performance metrics (algorithm efficiency and memory requirement) than currently used algorithms. Therefore, some adjustments within the current infrastructure have to be made. This can be as little as increasing the allowed sizes for public keys, ciphertexts, or digital signatures in software implementations. If a current system is under strict limitations, however, such a transition might also mean that hardware needs to be exchanged to allow for more space. We will elaborate on this topic in Sect. 4.4.

The second direction, *quantum cryptography*, also covers “quantum key exchange” or “quantum key distribution” (QKD). This technology uses principles of quantum physics similarly to but differently from quantum computers described in Sect. 1 in that it looks to use quantum computing for potentially interesting cryptographic advancements. It differs from post-quantum cryptography in that instead of being designed with the intention of protecting against a quantum adversary/quantum computer, it explicitly aims to apply quantum computing principles to creating new cryptographic techniques. Thus, quantum cryptography may, but also may not protect against a quantum adversary, as described in more detail below. In QKD, sent and received quantum states are essentially the “secret keys” that are then used to encrypt data using symmetric encryption. By the laws of physics, keys that have been eavesdropped on by attackers will not be received correctly anymore, thus implying that, if parties end up with the same key, an eavesdropper was not active.

While not designed to specifically counter a quantum threat, the design of QKD using quantum states makes it naturally resistant to the types of quantum attacks discussed earlier. Thus, QKD has also entered the space of terms referred to when looking at security against a quantum attacker. However, there is a subtle yet significant security gap to such claims that is often evaded when QKD is marketed as a solution to the quantum threat. Namely, QKD does not solve *entity authentication*. Colloquially, entity authentication is assurance that the party sending data is who they claim to be. Thus *data authenticity*, *data confidentiality*, and *key secrecy* are all reliant on first achieving entity authenticity—to show that data is confidential

to two parties, not manipulated, etc., one must first know that the other party is not impersonated. QKD does not solve entity authentication and is therefore reliant on classical methods of authentication. For example, geo-location of the intended communication partner must be both pre-established and so precise that it is impossible that another entity can impersonate them, or a cryptographic method for entity authentication must be used. Without such an added entity authentication solution, an attacker can impersonate communication partners or perform man-in-the-middle attacks. Cryptographic methods for entity authentication rely on one of two approaches: (1) a symmetric key or (2) an asymmetric key. In both cases, QKD relies on assumptions similarly to post-quantum algorithms.

In addition to the above considerations, QKD comes at the cost of physically building a new infrastructure that physically connects or provides line of sight between the end points. Moreover, state-of-the-art QKD systems either have a rather short range (approximately 100 km [7] with some experimental results extending to longer ranges [77]) or require “repeaters” to help relay the communication over longer distances. Unfortunately, such repeaters have a history of being vulnerable to attacks, casting an additional security concern for QKD in practice [7, 100]. Therefore, QKD seems to serve as a solution for certain applications, but not as a general protection suitable for all of tomorrow’s diverse security needs.

In the remainder of the chapter, we focus primarily on post-quantum algorithms vis-a-vis quantum cryptography, QKD, designing quantum computers, or quantum technology in general as we concentrate on transition strategies and challenges for hardening against a quantum threat. Notably strategies and challenges for use of quantum computing differ significantly from defense against such adversaries.

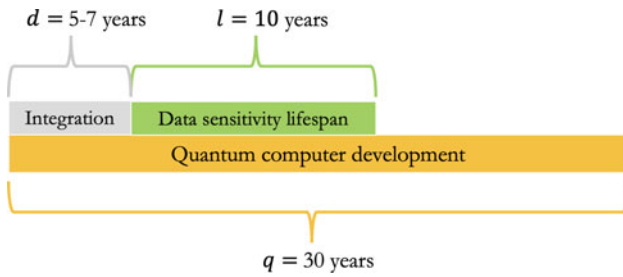
### 3.2 *Post-Quantum Transition Timeline*

The immense efforts in developing post-quantum alternatives have constituted a significant step in securing systems against a quantum attacker. However, as NIST itself states, “. . . it appears that a transition to post-quantum cryptography will not be simple as there is unlikely to be a simple ‘drop-in’ replacement for our current public-key cryptographic algorithms” (NIST, Call for submissions, 2017 [20]). This statement implies that, while NIST is standardizing foundational algorithms, that is merely the beginning of the transition. Further context must be accounted for *in addition to* use of post-quantum algorithms.

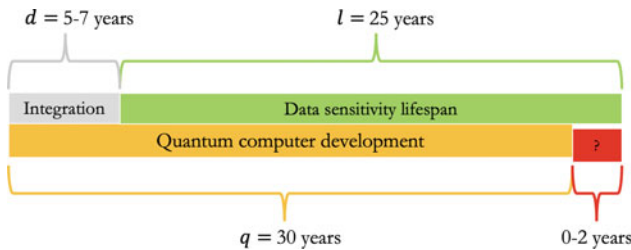
Combining development with back-tracking attacks, Mosca [65] illustrates the urgency of a post-quantum transition with a simple equation:

$$l + d > q,$$

where  $l$  gives the lifespan of the information that needs to be kept secret,  $d$  is the number of years needed to deploy post-quantum algorithms in the respective applications, and  $q$  corresponds to the number of years until cryptographically



**Fig. 2** Illustrated example of data sensitivity lifespan (green), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow). In the illustrated example, data sensitivity lifespan is relatively short compared to the development timeline for a quantum computer. In practice, it is unclear how many years duration can be assumed for the yellow timeline

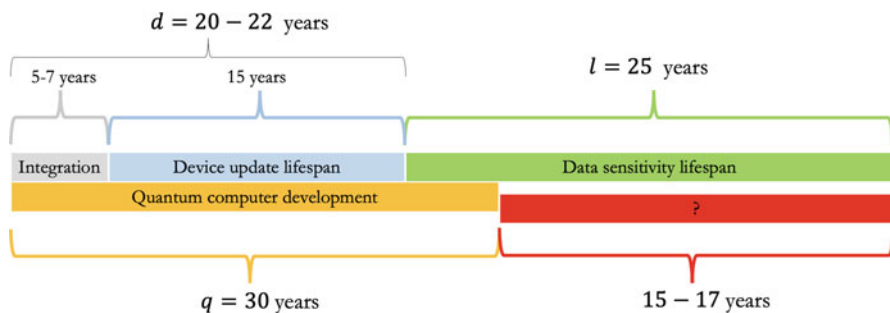


**Fig. 3** Illustrated example of data sensitivity lifespan (green), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow). In the illustrated example, data sensitivity lifespan implies that several years of data would be vulnerable (red) in the event of a quantum attack. Moreover, if back-tracking attacks are accounted for, all data in this illustration is vulnerable (the yellow component would need to be longer than the combined gray and green components to avoid such attacks). If the development timeline of a relevant quantum computer was less than 30 years, the amount of compromised information would be even greater

relevant quantum computers can be built. We visualize this using an example in Fig. 2.

In the illustrated example, system risk is low given an assumed quantum computer development timeline of  $q = 30$  years; under such an estimate, there would be sufficient lead time to plan for and integrate post-quantum cryptographic measures. However, the image oversimplifies the situation. Not only may an estimate of 30 years for development of a quantum computer be overgenerous, but the data sensitivity lifespans in some systems are well beyond 10 years. For the illustrated example in Fig. 3, if data sensitivity is, for example, 25 years, then even an assumption of a 30-year development timeline for a quantum computer is insufficient to protect data.

Mosca’s equation can be applied to calculate the urgency to start the post-quantum transition for an entire system’s public-key infrastructure, but it can also be used for estimations for specific applications. For the latter use-case, we would extend the equation by yet another variable,  $h$ , representing the lifespan used in the



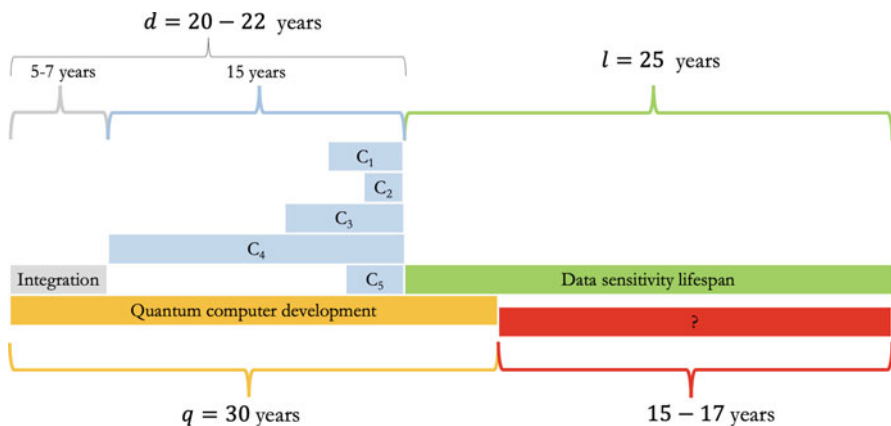
**Fig. 4** Illustrated example of data sensitivity lifespan (green), device lifespan as a function of the update frequency for internal cryptographic algorithms (blue), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow). In the illustrated example, consideration of update potential significantly increases the data-at-risk lifespan, and even without back-tracking attacks decades of data would be vulnerable in the event of a cryptographically relevant quantum computer. To protect against back-tracking attacks, the cumulative end of the gray/blue/green timelines would need to be earlier than the yellow quantum computer development timeline

device-to-be-transitioned. For example, if a cryptographic algorithm is implemented in hardware on a device and that device is then deployed in practical use,  $h$  could represent an extended period of time. If the algorithms are implemented in software, then updates may be more frequent; however, on the user end of the spectrum, smart yet “disposable” Internet of Things devices may never receive a manufacturer software update. In either of these cases, the available cryptographic algorithms are tied to actual device lifespan. If cryptographic algorithms were programmed in hardware for a system used in outer space, for example, that system may perform its entire intended functional purpose—lasting years—without an update to the cryptographic algorithms used.

Figure 4 illustrates a case such as described above, where a device has an extended lifespan of 15 years due to, for example, programming in hardware and the deployed device being inaccessible for updates (such as deployed in space). Due to an added 25-year data sensitivity lifespan and the risk of back-tracking attacks, post-quantum algorithms are employed. Thus, not only must the post-quantum algorithms required be developed prior to device deployment, but protocol development and integration must also take place (see Sect. 4). It is not possible to “drop-in” solutions without accounting for functional needs due to both the differences in post-quantum algorithm memory/computational cycle costs and potential needs for post-quantum protocols vs. algorithms. In this example, we see the quickly accrued time: a minimum of 45 years in the example. It is unclear when a cryptographically relevant quantum computer will be actionable; however, the entity responsible for a system would, in this example, either need to be confident that such a quantum computer is not actionable for 45–47 years, or assume all risk for the potentially substantial “red box” time period.

Cryptographic agility plays a notable role in the implications of the additional “blue” timelines in these figures. A system that is capable of regular updates will more nearly approximate Fig. 3. In fact, for many working in the cybersecurity sector who maintain full system control and are able to readily replace system components, the timeline shown in Fig. 4 may seem protracted; however, for various systems in government infrastructure, critical systems, defense sectors, and irregular environments (e.g., undersea, polar, and outer space), various components may be either hard to reach or were never intended to be replaced until the entire device expires. As such, systems being fielded now, even before post-quantum integration, should be carefully considered for cryptographic agility and the ability either to update the algorithms or retire the entire device if needed, to ensure that the “blue” device lifespan is minimized.

Figure 4 is illustrated as a single “device” with lifespan in blue; however, a typical system will include a multitude of components, some of which the system manager does not have an option to introduce post-quantum solutions to at a later date (e.g., commercial-off-the-shelf (COTS) devices with algorithms implemented in hardware). Within a system, the weakest link is a prime target for a cyberattack, and system information may be generated, shared, and acted upon by various components. Individual systems will vary, but a general guideline for a system’s *pre-quantum lifespan* is the longest common duration across all components. Even if most components are updated at a moderate frequency, the quantum risk to the entire system should thus be gauged on the weakest component, as illustrated in Fig. 5. For example, an aircraft may rely on several communication Systems links with different control components—for example, Global Positioning Systems (GPS),



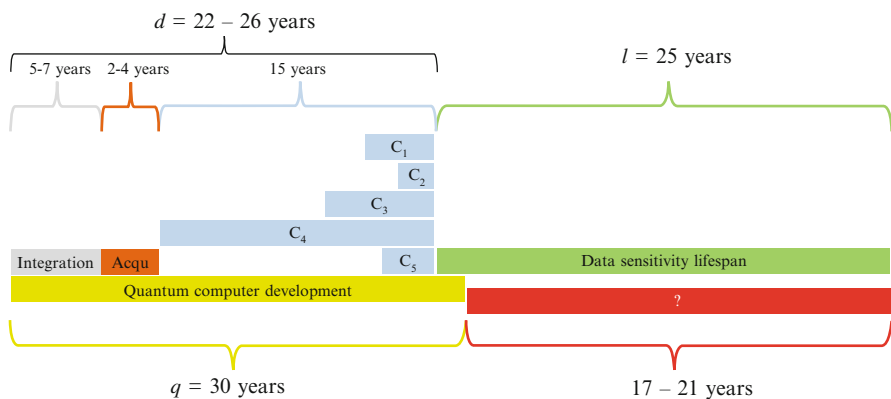
**Fig. 5** Illustrated example of data sensitivity lifespan (green), device lifespan as a function of the update frequency for internal cryptographic algorithms (blue), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow).  $C_i$  indicates the  $i$ -th component. In the illustration, there are five components in the system, with the pre-quantum lifespan of the system being dependent on the longest common component lifespan duration (here  $C_4$ )



radio communications, and ISR relays—each with a different manufacturer, and all contributing to the aircraft command and control. Each component may be on a different update schedule from its provider and require different types or degrees of quantum resistance. However, the entire aircraft is only quantum-resistant in its operation if all components are. Thus, if one aircraft component is quantum-vulnerable but is rarely updated or impossible to update without a major replacement cost due to legacy design, then that component contributes to a quantum-vulnerability for the whole system, regardless of whether or not other components are updated. Therefore, it is important to analyze the urgency of the post-quantum transition for smaller compartments as well as the entire systems to accurately estimate the time needed to deploy post-quantum algorithms to the entire system.

For more customized and protracted device designs, such as may be necessary for sensors in nuclear energy systems, proprietary system components, and other nonagile system components, this may prove to be an even greater risk due to procurement life cycles. For example, if a satellite system component is custom-made on a competitive contract for a government entity, then not only do the design, integration, and component lifespans factor into  $d$ , but the acquisition process timeline must also be accounted for. Figure 6 illustrates this consideration.

In conclusion of this section, it is important to emphasize that the point of time when to start to transition to post-quantum secure cryptography is not trivial. This holds in particular for large systems as these are only as secure as their weakest building block. Moving on, considerations during the post-quantum transition are discussed.



**Fig. 6** Illustrated example of data sensitivity lifespan (green), device lifespan as a function of the update frequency for internal cryptographic algorithms (blue), acquisition process timeline (orange), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow).  $C_i$  indicates the  $i$ th component

## 4 Post-Quantum Transition: Integration Considerations

Industry has taken action in response to the urgency of the quantum threat, and governments and defense sectors have begun to look at post-quantum options [22]. With many options available and various terminologies in use, a natural question for system designers is how to sort information and what considerations should drive decision-making regarding the post-quantum transition. In this section, we provide a cautionary note to the reader about certain technology categories advertised for quantum resistance and then turn our attention to example transition considerations for decision-makers to use when assessing system needs and options.

### 4.1 A Cautionary Note

Various companies have established new business models on offering post-quantum cryptographic solutions and more established companies have also added post-quantum cryptography to their offered services, capabilities, or features [1, 5, 47, 49, 52, 55, 59, 78–89, 103]. Distinguishing among such solutions and the appropriateness of them could be a challenge to system management. Furthermore, there is also the potential for “snake-oil” solutions to be marketed among actionable options, creating yet a more complex array to sort through. We provide a cautionary note on two types of claimed solution sets that may either not be generically appropriate or that may introduce unnecessary complexity to a system without coherent security gains. While it is not impossible that an appropriate solution could occur within one category or the other, system maintainers should carefully assess their threat model and needs before considering these.

#### Symmetric Techniques

Symmetric key cryptography has been in existence for centuries, with the Roman Caesar cipher being an early example. Thus, symmetric techniques have long predated the introduction of the asymmetric cryptographic techniques now threatened by quantum computing. Moreover, symmetric cryptographic techniques do not use the same underlying designs that make many current asymmetric cryptographic algorithms susceptible to quantum attacks; hence, currently, it seems that entire symmetric algorithms do not need to be replaced but rather only the key sizes used in them increased [61]. Therefore, it might seem tempting to resort back to systems relying only on symmetric cryptography. In what follows, we caution against this approach as it does come with downsides.

Since there is no means in a symmetric key protocol for two parties to establish a key using only public information, symmetric keys must either be pre-distributed or distributed by a trusted third party. This raises the question: *What third-party*

*should be trusted with knowledge of keys and therefore transmitted information?*

The security considerations are many; even if the third party is a vetted access entity, for example, a key distribution hub internal to a government entity, the nature of such a hub makes it also a high-value target and a single point of failure. If an adversary was ever able to gain access/hack-in/etc., they would also gain access to not one communication link's data, but an entire system of data in a single strike. Coupled with back-tracking attacks, such a third-party approach could be even higher risk if keys also are not changed frequently (providing a form of *forward secrecy*). Thus, even a vetted and self-contained third-party key management for symmetric keys not only lacks defense-in-depth, but is actually far weaker than most current cryptographic key infrastructures. When the third party is an external software provider, then not only does all the above apply, but there is an added risk stemming from that entity's access to the keys and consequently the potentially sensitive data being transmitted, for example, in a government or defense system.

Given the above, it may seem odd that some systems still use symmetric key management infrastructures. To understand this, we can examine an example of a common, modern protocol that still relies on symmetric key cryptography—the Kerberos protocol [72]. Kerberos is used, for example, in Microsoft Windows [104], which employs a Microsoft component as a trusted third party to provide keys to other Microsoft components. In Windows, Kerberos is used for example to support user single sign-on to allow access to a variety of Microsoft services. Thus, we see an equal-trust paradigm in this use of Kerberos; if a user is acting on their own (e.g., a laptop is accessing all Microsoft components within the laptop under their physical control), then trust in another Microsoft component to help manage that access does not substantially change the access risk. Thus, the choice of this symmetric key management and security thereof is highly dependent on the needs and security assumptions of the use-case.

When investigating potential post-quantum system solutions, it is thus advisable to be cautious of solutions that advertise quantum resistance but eschew use of public-key algorithms altogether. Such solutions may in fact evade the process of replacing current asymmetric cryptographic algorithms with post-quantum cryptographic alternatives by instead resorting to symmetric-only designs and “downgrading” system security to highly vulnerable trust infrastructures.

## **Mixing Quantum and Post-Quantum**

Another aspect worthy of caution is conflation of security properties offered by quantum cryptography with those of post-quantum cryptography. Section 3.1 discussed the intent of quantum cryptography and gaps in application to problems of quantum resistance. Notably, quantum and post-quantum cryptography describe two very different subfields of research and are even designed with different fundamental requirements (i.e., post-quantum cryptography can run on a classic computer whereas quantum cryptography is designed for a computer supporting quantum

mechanics). Thus, solutions claiming a mixture of these terms and guarantees should be considered with caution.

Ultimately, when a system maintainer selects a solution it should be based on the particular system's needs—both in terms of security and threats. Failure to do this can lead to use of solutions that cause unnecessary computational cost, memory cost, physical space and weight, or even simply product cost. In this context, and considering the mixed goals and design requirements of post-quantum cryptography and quantum cryptography, managers should carefully assess whether such a solution provides their particular system any security benefits over a more streamlined post-quantum solution.

## 4.2 Confidentiality vs. Authenticity

As mentioned earlier in the chapter, *confidentiality* and *authenticity* are two of the core security guarantees that cryptography can provide. Section 3 looked at data lifespan as a consideration factor for post-quantum transition, and we can take a closer view at the implications for each of these two guarantees under a quantum threat. Each guarantee may have a different sensitivity lifespan and each is dependent on the use-case, hence it is critical to assess system goals when undertaking a post-quantum transition.

*Confidentiality* is the guarantee that an adversary cannot *read* or *eavesdrop* on transmitted data. Whether such data is sensitive mission data, proprietary information, critical infrastructure planning data or daily monitoring levels, or even simply email contents, each type of information has a different lifespan. Sensor data, for example, temperature readings, may have a relatively short lifespan. If an adversary was to learn thermostat readings in 10 years then, even with a back-tracking attack, the information may not be particularly useful. If the lifespan is short, then there is more leeway time for post-quantum integration (at least for algorithms and protocols affecting confidentiality). In contrast, the criticality of an early post-quantum transition for, for example, classified information transition may be higher. Government, legal, and other higher-profile systems regularly handle sensitive information of a longer lifespan or data that, if decrypted even several years later, could be aggregated for malicious effects. Such data can, for example, have a 25-year lifespan [45], with back-tracking attacks based on this lifespan shown in Sect. 3.

There is also a middle ground of information sensitivity. For example, the 2014 hack on Sony Pictures released emails, information on planned films, personal data, and salary information [39]. Suppose that such a hack took place using a quantum computer, for example, 10 years after the emails, personal information, and information on planned films was sent and that the adversary employed a back-tracking attack to decrypt all the data. Perhaps 10 years after the fact a planned film would already be made, thus expiring the sensitivity of the information. However, personal information would still be actionable. Moreover, email content could

expose the company to lawsuits and salary information could make individuals financial targets. If that hack was 5 years or 15 years after time-of-send, the sensitivity of each of these data types might range from expired to very sensitive. In short, the type of information sent across a communication channel and potential malicious uses of it must be weighed to identify the urgency of post-quantum need for that channel or use-case.

In contrast to confidentiality, *authenticity* is a term usually applied to two aspects within cryptography: *data authenticity*, which is also often referred to as *integrity*, and *entity authenticity*.

*Data authenticity*, a.k.a. *integrity*, refers to a malicious actor's ability to modify, forge, or otherwise manipulate data. Digital signatures (asymmetric algorithms vulnerable to a quantum adversary) are often used in, for example, S/MIME email signatures as well as web connections and even credit card payments (see [24, 69] for a good overview). In terms of lifespan, a quantum adversary that is able to break a signature key in the future and retroactively forge a transaction or web connection that occurred several years prior may have little gains; thus, in many cases, people argue that post-quantum transition of data authentication algorithms is less important than encryption. However, such arguments depend on the perspective. For example, a user may not be concerned about forgery of grocery receipts when a payment card is already expired, but the legal system's reliance on such digital proofs against forgery takes on higher risks.

Consider, for example, a land ownership document that is digitally signed, for example, through DocuSign [99]. If an adversary was able to break a digital signature on the land deed years after transfer of property, they may successfully create a case to contest ownership—or to argue ownership by multiple entities. Similarly, the legal implications of signing contracts and various government documents rely heavily on the unforgeability of such documents long into the future. To use other terms, a quantum adversary using back-tracking attacks could subvert auditability or nullify the validity of audits. Thus, data authenticity must also be considered relative to the use-case needs and the required auditability lifespan, for example, matching the green box in Fig. 4.

*Entity authenticity* refers to protections against impersonation (“forgery of identity”) vice data forgery. For example, when connecting to an online bank, a user wants to have a guarantee of the legitimacy of the bank's website in order to avoid identity theft and the bank wants to have a guarantee of the user's identity, to avoid liability of impersonation to access funds. Frequently, this is seen as a much shorter “lifespan” interaction—if a viable quantum computer against the cryptographic aspects becomes a reality (e.g., 10 years after a banking log-on), the risk to that transaction is minimal. Entity authentication, however, is also tied to data authenticity, in that forgery of the entity calls into question validity of the data. In many cases, identities are tied to a *Public Key Infrastructure (PKI)*. Under PKI, some trusted third-party certificate authority uses digital signatures to sign off on certificates to link an identity to a public key. Thus, if the authority's key itself is obtained by a quantum adversary, that adversary can impersonate various identities as well as forge data by them. Again, if we are assuming back-tracking

attacks for some future quantum adversary, then these forgeries are “after the fact.” Nonetheless, the scale of damage that an adversary may achieve in terms of legal and audit validity effects is many orders of magnitude larger when they are able to attack the third-party certificate authority in contrast to only one end-user. A natural solution to this problem may appear in the form of transitioning the certificate to using a post-quantum algorithm—even if the end-user digital signature is standard, then at least it is not possible for an eventual quantum adversary to retroactively create competing identities. Unfortunately, this solution is inhibited in that current systems must be able to validate the certificate authority’s signature on a certificate; therefore, ironically, the certificate authority’s algorithm may be the last to be upgraded as legacy systems need to recognize it. Thus, we see that there is a larger infrastructure around achieving post-quantum data authenticity that takes time to transition, creating an urgency to do so that may not be immediately apparent. In Sect. 4.5, we will discuss post-quantum *hybrid* techniques that may help solve the legacy challenge.

### 4.3 *Protocols vs. Algorithms*

In cryptography, protocols and algorithms are interdependent but separate concepts. For example, encryption is a cryptographic algorithm—a function—than, on input of keys and data, provides a ciphertext output. An example of a cryptographic protocol includes key exchange protocols—interactive steps between parties for establishing the key that is then used for encryption. Other examples include mutual authentication protocols such that parties are protected against impersonation within the channel, consensus protocols, and privacy-preserving protocols, to name a few. In the case of data encryption, the security of the encryption algorithm is directly reliant on the security of the key exchange protocol used to establish the encryption key. If the latter breaks and an adversary could obtain the key, then it will also be able to decrypt information that it should not have access to. Protocols are used in most aspects of daily life, including to secure digital communications to banks, smart door locks, car keys, pacemakers, among Internet of Things devices, etc. This raises a question: when identifying quantum resistance measures for system hardening, should post-quantum secure techniques be applied to the algorithm, the protocol, or both?

Security of even the most simplistic of systems relies on cryptographic protocols to combine algorithms in dependable and resilient ways. Algorithms can be used as “building blocks” for secure protocols. For example, version 1.3 of the Transport Layer Security (TLS) protocol combines cryptographic key derivation functions, message authentication codes, and digital signatures, among others. Even if the underlying components are strong, they could be combined in such a way that the resulting protocol is broken and the adversary learns the secret information. Thus, having post-quantum algorithm subcomponents is necessary for the post-quantum security of the protocol, but not sufficient to automatically imply that the overall

protocol is secure, and analysis of the protocol itself must be considered. Finally, protocol security is dependent on the threat model of the system (i.e., what it is trying to protect against) and this frequently extends to many other threats than just quantum computing. Some protocols are being created or adapted that may be suitable for post-quantum applications [15, 16, 21, 26]. Other protocols that are already tailored for efficient and secure use inside of a given system may require a re-tailoring with post-quantum algorithm subcomponents to assess suitability against both a quantum attacker and the system's current core threat model.

In summary, the answer to the above question is that it is not sufficient to simply replace quantum-vulnerable cryptographic algorithms—the entire protocol needs to be analyzed and potentially changed to achieve overall protection against quantum adversaries.

#### ***4.4 Software vs. Hardware***

As explained in Sect. 3, the number of years needed to deploy a system is determined by the time of integration, the acquisition process, and the device lifespan, at a minimum. The latter two are particularly important if hardware needs to be replaced. For example, for communication between aircraft or vehicles, messages are authenticated using digital signatures and then broadcast (see Sect. 5.2 for a detailed description of aircraft communication systems and [48] for a current vehicle-to-vehicle communication standard). In high-traffic areas, this means that aircraft or vehicles might need to verify hundreds of signatures. Hence, dedicated hardware chips that implement the verification algorithm are often integrated in the aircraft or vehicles to improve efficiency over software implementations. During a post-quantum transition, post-quantum algorithms must first be implemented and tested for the needed hardware processors, and then these dedicated chips must be manufactured and deployed in systems. There are a few works on how to reuse dedicated hardware chips for classical algorithms for a post-quantum algorithm. For example, [3] describes how to reuse RSA processors for transition to the lattice-based scheme Kyber. However, whether this is possible depends very much on the hardware as well as on the specific cryptographic algorithms being used.

This means that if a system includes dedicated hardware implementations for cryptography algorithms, the urgency to analyze the system regarding the need for a post-quantum transition is increased. Urgency also increases with the scale of the application. For example, while replacing one Automated Teller Machine (ATM) with an ATM that has been upgraded to be post-quantum secure may be a relatively feasible process, replacing all 470,135 ATMs in the United States. [4] requires an immense effort both in timescale management and financial investment.

In contrast, upgrading software is presumably easier as in most cases no hardware changes need to be made. However, the effort arising from potentially many dependencies in software libraries should not be underestimated. Further, many different companies make ATMs that may require many different software upgrades to transition all ATMs to post-quantum security options.

## 4.5 *Classical/Post-Quantum Hybrid Algorithms*

The urgency to switch to post-quantum secure cryptographic alternatives that has been described in this section is opposed by the uncertainty of whether post-quantum algorithms are secure. Cryptographic algorithms are naturally a high-value target for attackers due to the information advantage, with second-order effects from breaking an algorithm including financial and strategic impacts. Thus, cryptographic algorithms, whether classic or post-quantum, receive an intense degree of scrutiny, cycling through phases of uncertainty, breaks, and hardening revisions. Among the NIST post-quantum candidates, some algorithms have a fairly long history of testing, such as hash-based signature schemes (e.g., XMSS [44]), which are already recommended by the German Federal Office for Information Security [32], or the code-based Key Encapsulation Mechanism (KEM) McEliece [8]. The security of these is therefore more thoroughly vetted than some of the newer alternatives that are also up for standardization. For example, Rainbow [25] is a post-quantum algorithm invented in 2004 that has made it through three rounds of the NIST post-quantum standardization effort. Nonetheless, in 2022 research emerged that demonstrated significant vulnerabilities in Rainbow [11, 27], leading to key recovery attacks.

While it may be enticing to forgo newer algorithms in favor of those with more history to increase the likelihood of sudden security breaks, there is no guarantee that such time maturation provides indication of security—historically ciphers that have been thoroughly cryptanalyzed for many years have also been identified as holding new vulnerabilities [14, 68]. Second, newer algorithms can provide different features than some of the more established variants. In post-quantum cryptography, there are usually trade-offs in memory or computational requirements, and for some applications the current algorithms possessing a longer history may not be suitable. Finally, the urgency for a post-quantum transition may prohibit a longer waiting period for more results to emerge.

As a solution to this predicament, hybrid or composite algorithms [12, 13, 75, 96] have been suggested that have also been recommended by standardization agencies such as NIST [18], the German BSI [32], European Telecommunications Standards Institute (ETSI) [28], and the Internet Engineering Task Force (IETF) [23]. *Hybrids* refer to the combination of two or more algorithms of the same kind. For example, a *hybrid digital signature* may consist of a combination of two underlying digital signatures. Hybrids can be achieved by either combining classical (i.e., quantum-vulnerable) with post-quantum secure algorithms or combining different post-quantum algorithms of the same kind. The former approach aims to leverage security guarantees from classic algorithms that are well-understood but quantum-vulnerable while combining those with post-quantum guarantees. Such hybrid algorithms are post-quantum secure (if analyzed for that goal) and may also support backwards compatibility in some cases (e.g., a system that is not set up to verify the post-quantum component may still verify the classic component). In contrast, the latter approach of hybridizing two post-quantum algorithms aims to decrease the likelihood of a successful attack by spreading security across different types



of assumptions (e.g., digital signatures designed based on different computational hardness assumptions).

As with selecting whether to post-quantum transition individual algorithms (e.g., encryption, digital signatures, etc.) and protocols based on system security requirements, the use-case needs should be assessed when considering use of hybrids. Hybrids do generally come at a higher performance cost, so use may be best as a stop-gap solution during post-quantum transition or where the potential security benefits outweigh the overhead. Thus, it may be important for a system to have, for example, a hybrid key encapsulation mechanism to ensure extra security for the key distribution both under a classic and quantum adversary while only requiring, for example, a classic digital signature. Generalization of such system requirements would be ill-advised and instead the transition strategy should account for individual system use and security guarantees required.

## 4.6 *Considerations Summary*

In summary, the following considerations are important when analyzing whether or not—and when—a post-quantum transition for a system is necessary.

The first and most important question to ask is whether the system might be vulnerable to a quantum attack. This can be analyzed by answering the following question formulated by Mosca and Mulholland [63]: “Does my [system] rely on asymmetric cryptography to encrypt information, provide data integrity, or for cryptographic key distribution?” If the answer is no, no further action is needed. If the answer is yes, the next important step is to analyze the urgency of the needed transition.

As we explained in detail above, the urgency is defined by the data sensitivity lifespan—how long the communicated data needs to be secure—and the number of years needed to deploy quantum-secure alternatives. The latter can be further determined by considering the integration time, the acquisition time (of, e.g., requisite hardware), and the device lifespan of the devices used in the system. All three of these depend, on the one hand, on how crypto-agile, and therefore on how easy to change, the system’s building blocks already are. On the other hand, they also depend on whether the system update would include changing hardware or only software (see Sect. 4.4). To analyze the data sensitivity lifespan, in particular two security goals need to be considered: how long does the data need to be confidential and/or how long does the data need to be authenticated (see Sect. 4.2).

In addition to determining the urgency of the needed transition, an important question to answer is also whether the quantum-vulnerable algorithms should be switched by post-quantum algorithms or by (classical/post-quantum) hybrid algorithms (see Sect. 4.5). Reasons to do the latter could be, for example, to diversify security risks (i.e., to avoid a sudden break of a single algorithm) or to enable backward compatibility with post-quantum unaware parts of the system. It is important to emphasize that not only might replacement of quantum-vulnerable

algorithms with quantum-secure algorithms be needed, but additional changes to the protocol or system as a combination of such algorithms might also be essential (see Sect. 4.3).

## 5 Case Studies in Quantum Risk and Transition for Critical Systems

Many systems critical to modern life require cryptography to safely and securely operate. For instance, critical infrastructure such as the power grid, water utilities, healthcare systems, transportation infrastructure including the physical built infrastructure, ground vehicles, ships, aircraft, defense systems, and many other such systems and SoS heavily rely on keeping data secure [66]. Eavesdropping on command and control (C2) and ISR data from UASs used as part of national defense could allow for an adversary to gather sensitive intelligence data that puts a nation's security at risk. This includes eavesdropping on encrypted data traffic and performing a back-tracking attack years later by quantum adversaries as described in Sect. 2.1.

This section discusses the potential risks to critical systems in a quantum-computing era through the lens of some example analyses to understand when post-quantum upgrades and overhauls to existing and future systems must occur. More concretely, we consider case studies in medical devices, satellite systems, aircraft SoS, and finally nuclear power plants.

It is important to note that while there is strong advocacy that the analysis shown in Sect. 3 should be conducted, that analysis is explicitly excluded below. The reason is that the data necessary to conduct the analysis across the examples shown in this section is generally proprietary and confidential in nature, and resides with companies that manufacture the systems discussed. In some examples, the relative urgency is discussed for a system to implement post-quantum cryptographic solutions but this is only general information and in practice may be different for specific systems of concern.

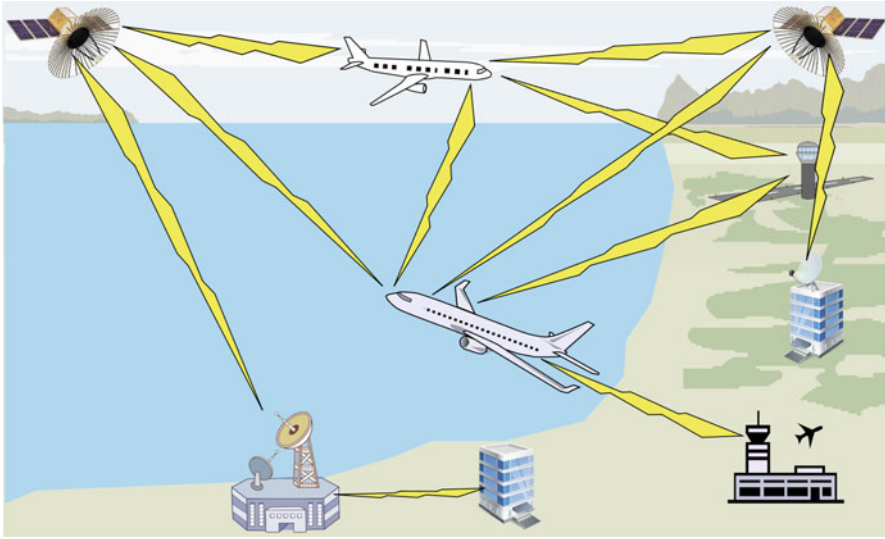
### 5.1 Medical Systems

As noted analogously for the cryptographic layer, system implications of a quantum attacker vary across system designs, data lifespan, and data sensitivity. Many types of data a system may have are only relevant for a brief period of time such as throttle position data transmitted across a vehicle's controller area network (CAN) bus. Other types of data such as ISR data collected by a defense system may be sensitive for many years. Further, as discussed in Sect. 2, data aggregation can lead to back-tracking attacks.

An example of a continuous positive airway pressure (CPAP) machine demonstrates data sensitivity lifespan of the hardware. CPAPs are often expected to last three to five years of nightly use by patients at home. A typical development cycle for a new generation of CPAP machine can take several years and may reuse significant system elements from previous CPAP generations. Corresponding to Fig. 6, the lifespan of data is  $l = 50$  years under, for example, the old U.S. Health Insurance Portability and Accountability Act (HIPAA) (and now indefinite) [29]. Moreover, the deployment time  $d$  must additionally account for reused system elements, integration, and acquisition such that the data is post-quantum safe in the event of a quantum attacker. Note that even under an unrealistic but ideal scenario of  $d = 0$ , the fact that  $l = 50$  or more years necessarily puts intense pressure on medical providers. If a cryptographically relevant quantum computer is viable in  $q < 50$  years, then providers not using post-quantum secure options today would be in violation of HIPAA compliance for current data, given the reality of back-tracking attacks.

## 5.2 Aircraft System of Systems

A crewed aircraft SoS is comprised of ground control (air traffic control, airport ramps, maintenance facilities, airline logistics and management, etc.), two-way audio and digital communications (direct digital and analog radio communications and digital radio communications via satellite relay), anticollision systems (traffic collision avoidance system, ground proximity warning system, automatic Dependent Surveillance–Broadcast system, etc.), the crew (pilot, co-pilot, etc.), passengers and associated systems (i.e., in-flight entertainment system), and the aircraft itself (avionics, engines, fuel management system, control surfaces, etc.) [64]. As such the crewed aircraft SoS contains many digital systems to communicate with the ground, to other aircraft, to internal aircraft systems, among the crew, and to entertain the passengers. Many of the digital systems aboard the aircraft are linked via a data bus (ARINC 429, AFDX, MIL-STD-1553, etc. [35]). Some passenger-accessible systems such as the in-flight entertainment systems could be attack vectors to sensitive aircraft systems [30, 107]. When modern, “smart” aircraft supporting Wi-Fi are considered, we can look at WPA3—the latest of the Wi-Fi connection standards. WPA3 relies on asymmetric techniques within the Dragonfly handshake [41, 46, 102], making it vulnerable to quantum attacks. Transitioning such systems to use post-quantum techniques would be a longer process since transition for aircraft components must be accounted for in addition to any upgrades of the supported standards outside of the aircraft environment [64, 93]. On the ground, aircraft often digitally interface with maintenance equipment to run diagnostics, download prognostics and health management data from major aircraft subsystems, and upload data to the aircraft such as navigation information and updates to critical flight systems [94]. Figure 7 provides a simplified CONOPS of the aircraft SoS.



**Fig. 7** Crewed aircraft SoS. The aircraft communicates with two satellites to provide (1) in-flight positioning data and telemetry back to a central office, and (2) in-flight live entertainment and Internet access to passengers. The satellites feed data to/from ground stations. Digital and analog links with other aircraft and regional airports allow for two-way communication

Beyond geolocation and other satellite links, communication links also connect aircraft-to-aircraft and aircraft-to-ground stations. For the latter, a modern air traffic management system that uses mutual entity authentication and key agreement based on classical cryptography has been recently introduced [70]. Similarly, it can be expected that future secure aircraft-to-aircraft communication will need to verify digital signatures to check the authenticity of the sending craft or system, to, for example, avoid spamming attacks, where a system’s capacity is actively overloaded to force system failure. Given the large number of aircraft that are in transmission range of another aircraft at a given time, large numbers of signatures would need to be signed and verified every second. For instance, an aircraft flying over the Los Angeles Basin or a similar congested airspace at a higher flight level (FL) such as FL330 or above (33,000 feet or above) might receive Automatic Dependent Surveillance—Broadcast (ADS-B) data from hundreds of other aircraft in its communication range (although not all may be displayed on an ADS-B receiver due to the typical  $\pm 3500$  feet 30 nautical mile “hockey puck” data filtering based on aircraft position [31]) where each aircraft sends a burst of data every 0.5–10 seconds. Hence, it is expected that dedicated chips would be needed to do such cryptographic operations on board the aircraft (an aspect that further hampers post-quantum transition as explained in more detail in Sects. 3.2 and 4.4). A quantum adversary breaking the authenticity or integrity of this communication might be able to change messages to cause mid-air collisions and other high-risk situations. If a quantum adversary could break confidentiality, it would be able to read potentially

sensitive message data either to the aircraft or to entities on-board, creating a potential security risk, for example, in the case of a non-commercial aircraft such as government or defense-related aircraft.

Moving closer to the ground, a quantum adversary could be able to forge digital signatures that should otherwise guarantee the authenticity and integrity of software updates of any of the avionics or control systems. Such software updates are done routinely during maintenance and could cause disturbances during the flight, and in the worst case, cause the aircraft to crash (in back-tracking attacks, an adversary could also tamper with evidence and auditability).

Inside the aircraft, a (very powerful) quantum adversary could be able to also break confidentiality or integrity of the communication on the aircraft itself, for example, between the cockpit and control surfaces such as the wing flaps or between the cockpit and the engine. The data buses inside the aircraft provide a potential avenue of intrusion. For example, an adversary can collect traffic and take it offsite to a quantum computer to extract information (breaking confidentiality and/or integrity) to learn operational information and gain long-term authentication keys. Once keys are derived via quantum cryptanalysis, the adversary would be able to return to the aircraft proximity and potentially take over control of data buses and communication links between the cockpit and, for example, the engines.

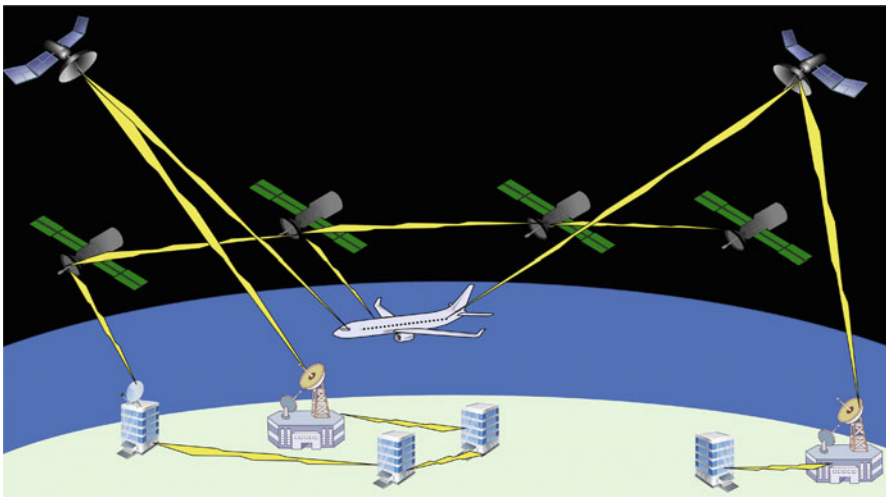
### ***5.3 Satellite Systems***

As mentioned in the crewed aircraft SoS in Sect. 5.2, satellites provide important communications links. Satellites communicate with aircraft for a variety of purposes such as global satellite navigation (GPS, Global Navigation Satellite System (GLONASS), Galileo, BeiDou, etc.) [71], two-way data for a variety of avionics and crew-ground communications systems (prognostics and health management data for key aircraft systems such as engines, messages to the crew or to the ground pertaining to aircraft operations and notices to aviators, weather reports, etc.), passenger in-flight entertainment system live feeds, passenger Internet access, and others. Back-haul data may constitute such relays for ground stations/aircraft, but also refer to data relayed, for example, across a network of satellites. Satellite system use extends well beyond geolocation and back-haul data applications. Namely, the ability to support such features comes with the need to maintain management of the satellite systems themselves, that is, C2. Naturally, this requires security of the C2 connection for all other features and capabilities to be maintained. With a variety of space systems and communication technologies comes a variety of device lifespans and therefore quantum threat vectors. The system layers and interconnections point to a variety of timeline considerations and post-quantum transition decision point implications.

Some satellites are part of low earth orbit (LEO) constellations that are replaced frequently (every 3–5 years) while other satellites may be in geostationary (GEO) orbits with long lifespans (of 15 or more years). In almost all cases, the hardware

on satellites that is launched into orbit is not field serviceable and remains with the satellite throughout its life. Many satellites have hardware encryption solutions although some may have software encryption solutions that can be updated within the limits of the hardware [6]. In most cases, satellites talk to many different systems—not just aircraft. The satellite transceivers that a satellite uses may be many years old or may be brand new. Also in many cases, satellites must still be able to communicate with legacy transceivers using outdated cryptography. There may be many transceivers that are located in remote areas or are inaccessible so that upgrades cannot be done. When a system is forced to support old cryptographic techniques, downgrade attacks become more likely. All such considerations—difficulty to transition systems and backward compatibility risks—must be accounted for in the system transition plan and post-quantum strategy transition timeline. Hybrid algorithms (described in Sect. 4.5) might offer a way to support older cryptography but also enable security guarantees of post-quantum solutions.

Some satellites may route communications across a back-haul between the transceiver aboard an aircraft and a ground station, as illustrated in Fig. 8. Satellites may have a data link to one or several large ground stations where data is then forwarded to recipients via the Internet, private networks, or other means. Sometimes ground stations are also located in remote regions and are teleoperated, adding yet a further factor into the system diagram of post-quantum transition links. Figure 8 shows a simplified configuration of satellites, ground stations, aircraft, etc.



**Fig. 8** Satellite CONOPS. A LEO satellite constellation maintains continuous communications with the aircraft and passes data via a back-haul between the satellites to a data link with a ground station that then passes two-way data between the aircraft and a user through the Internet. Two separate GEO satellites communicate with the aircraft and directly to ground stations that relay the communications via the Internet and private networks to users

## 5.4 *Nuclear Power Plants*

Most modern nuclear power plants use analog controls for safety-critical systems but digital instrumentation and control (I&C) is coming to some existing plants as well as to-be-constructed plants [42]. Nuclear power plants generate energy from a nuclear fission process—normally via producing steam to spin turbines that generate electricity. In most western nuclear power plant designs, water is used to keep the nuclear fuel rods below 1200°C, which is the point where the zirconium cladding used on most fuel rods begins to decay and can generate hydrogen that produces an explosion risk, and also can lead to the release of radioactive particles into the primary coolant loop [67, 105]. Many sensors are placed throughout a nuclear power plant to monitor all plant systems and help operators to regulate the nuclear reaction taking place in the core. Naturally, safety is essential for a nuclear power plant and any security risks to that are necessarily extremely serious. The safety-critical I&C systems in a nuclear power plant are generally triple redundant to mitigate safety risk. As plants transition legacy systems to digital C2, or even just to digital sensors, the security of such communication links becomes a primary critical protection point.

While the core consideration for many systems is on security transition to post-quantum and matching current system risk profiles to security properties, extreme legacy systems such as nuclear power plants are new to the digital communication space and often currently lack any security protections. As such, there are both benefits and risks to designing for transition now. Potential benefits include the flexibility to design for post-quantum requirements (e.g., key sizes or computational resources) that may eventually be required, especially if any C2 will eventually occur over the air in years to come. Unlike, for example, Internet connections that must be adapted for post-quantum support and integration, such legacy systems are prime for customization at the initiation of security design. On the risk side, however, comes failure to observe the lessons learned in past infrastructure modernization. The Internet of Things is one such example, where previously unconnected devices were “upgraded” to modern connectivity; such connectivity both enabled better command and control of the devices but also introduced security risks—some of which were not well anticipated and planned for [34, 43, 60, 108]. Another issue with nuclear power plants and similar critical and heavily regulated infrastructure is the lengthy review process that must be conducted before changes can be made to core safety systems. Implementing digital I&C within a nuclear power plant may take 10–20 years, and any future changes to I&C systems such as to upgrade to post-quantum cryptographic solutions may take as much or more time. Thus, for legacy systems such as nuclear power plants that are being upgraded now, the core question is, “What current and future threats are being planned for?” When it comes to a quantum threat, the planning and transition timeline is essential.

Concluding this section on case studies regarding the quantum threat and the post-quantum transition, it is important to emphasize that there is a high risk in timelines for the post-quantum transition. This is, in particular, due to only



partial analyses of SoSs by concentrating on some but not all components. Fuller system analysis, such as is done for other risks [40, 73, 74], must proactively undertake inclusion of the quantum threat, with follow-on and urgent actions taken for vulnerable systems. However, this also presents an opportunity; quantum adversaries can be accounted for now in the fundamental threat model base-lining for systems being designed or fundamentally redesigned over the next decades.

## 6 Conclusion

Quantum computers are an impending threat on the horizon. While the exact timeline of a cryptographically relevant quantum computer is unknown, the consequences for classic asymmetric cryptography would be severe. As system managers and strategic decision-makers consider whether or not to transition to post-quantum secure alternatives, and potential timelines for transition, there are a multitude of factors to consider. Among these are legal and economic implications, system dependencies through data transit of multiple C2 links, the types of security guarantees needed (such as confidentiality and/or integrity), the types of system components needed (hardware processors or software updates), and the integration timeline with respect to data lifespan, post-quantum integration, acquisition, and device lifespan. All of these must be juxtaposed with the wager management takes on for development time of a cryptographically relevant quantum computer—a threat that could become reality in a couple of years, 15 years, 30 years, or any estimate to be placed for risk analysis. What is certain is that a strategic plan is required. Instead of ad hoc decisions limited to the cryptographic layer and subject to the winds of advertisement and marketing jargon, a true system transition plan is based on aggregated security needs and threat risks required for an integrated system in its entirety.

## References

1. agnostiq: A Workflow Orchestration Platform Designed for Quantum & HPC (2022). <https://agnostiq.ai/covalent/> [Accessed: 2022-03-29]
2. Alagic, G., Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.K., Miller, C., Moody, D., Peralta, R., et al.: Status report on the first round of the NIST post-quantum cryptography standardization process. US Department of Commerce, National Institute of Standards and Technology (2019)
3. Albrecht, M.R., Hanser, C., Höller, A., Pöppelmann, T., Virdia, F., Wallner, A.: Implementing rlwe-based schemes using an RSA co-processor. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**(1), 169–208 (2019)
4. An, L., Baynard, C., Chatterjee, C., Loh, C.P.A.: The locational study of atms in the u.s. by ownership (2018). [https://www.akleg.gov/basis/get\\_documents.asp?session=31&docid=22687](https://www.akleg.gov/basis/get_documents.asp?session=31&docid=22687) [Accessed: 2022-03-29]



5. Anhui Qasky Quantum Technology Co. Ltd.: Qasky (2022). <http://www.qasky.com/> [Accessed: 2022-03-29]
6. Banu, P.S.R.: Satellite on-board encryption. Ph.D. thesis, University of Surrey (UK) (2007)
7. Bäuml, S., Christandl, M., Horodecki, K., Winter, A.: Limitations on quantum key repeaters. *Nat. Commun.* **6**(1), 1–5 (2015)
8. Bernstein, D., Chou, T., Lange, T., von Maurich, I., Misoczki, R., Niederhagen, R., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Wang, W.: Classic mceliece. Tech. rep., Submission to NIST's Post-Quantum Standardization (2019).
9. Bernstein, D.J.: Introduction to post-quantum cryptography. In: *Post-Quantum Cryptography*, pp. 1–14. Springer, New York (2009)
10. Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.): *Post-quantum cryptography. Mathematics and Statistics* Springer-11649; ZDB-2-SMA. Springer, New York (2009)
11. Beullens, W.: Breaking rainbow takes a weekend on a laptop. *Cryptology ePrint Archive, Report 2022/214* (2022). <https://ia.cr/2022/214>
12. Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., Stebila, D.: Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. In: J. Ding, R. Steinwandt (eds.) *Post-Quantum Cryptography—10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 Revised Selected Papers. Lecture Notes in Computer Science*, vol. 11505, pp. 206–226. Springer (2019)
13. Bindel, N., Herath, U., McKague, M., Stebila, D.: Transitioning to a quantum-resistant public key infrastructure. In: T. Lange, T. Takagi (eds.) *Post-Quantum Cryptography—8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26–28, 2017, Proceedings. Lecture Notes in Computer Science*, vol. 10346, pp. 384–405. Springer (2017)
14. Boneh, D.: Twenty years of attacks on the rsa cryptosystem. *Not. AMS* **46**, 203–213 (1999)
15. Bos, J.W., Costello, C., Naehrig, M., Stebila, D.: Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In: *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17–21, 2015*, pp. 553–570. IEEE Computer Society (2015)
16. Brendel, J., Fiedler, R., Günther, F., Janson, C., Stebila, D.: Post-quantum asynchronous deniable key exchange and the signal handshake. In: G. Hanaoka, J. Shikata, Y. Watanabe (eds.) *Public-Key Cryptography – PKC 2022*, pp. 3–34. Springer International Publishing, Cham (2022)
17. Cabinet Office, U.G.: Government Security Classifications May 2018. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/715778/May-2018/Government-Security-Classifications-2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018/Government-Security-Classifications-2.pdf) (2018). Accessed: 2022-03-27
18. Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D.: Nistir 8105 report on post-quantum cryptography. Tech. rep., National Institute for Standards and Technology (NIST) (2016)
19. Chen, L., Moody, D., Liu, Y.K.: Post-quantum cryptography. Tech. rep., National Institute of Standards (NIST) (2016)
20. Chen, L., Moody, D., Liu, Y.K.: Post-quantum cryptography calls for proposal. Tech. rep., National Institute of Standards (NIST) (2017)
21. Crockett, E., Paquin, C., Stebila, D.: Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH. *Cryptology ePrint Archive, Report 2019/858* (2019). <https://ia.cr/2019/858>
22. Csenkey, K., Bindel, N.: Post-quantum cryptographic assemblages and the governance of the quantum threat (2021). <https://doi.org/10.31235/osf.io/3ws6p>
23. Gueron, S., Stebila, D., Fluhrer, S.: Hybrid key exchange in tls 1.3, internet draft. Tech. rep., Internet Engineering Task Force (IETF) (2022)
24. Degabriele, J.P., Lehmann, A., Paterson, K.G., Smart, N.P., Strefer, M.: On the joint security of encryption and signature in EMV. In: O. Dunkelman (ed.) *Topics in Cryptology—CT-RSA 2012—The Cryptographers' Track at the RSA Conference 2012, San Francisco, CA, USA, February 27–March 2, 2012. Proceedings. Lecture Notes in Computer Science*, vol. 7178, pp. 116–135. Springer (2012)

25. Ding, J., Chen, M., Petzoldt, A., Schmidt, D., Yang, B., Kannwischer, M., Patarin, J.: Rainbow. Tech. rep., Submission to NIST's Post-Quantum Standardization (2020)
26. Dowling, B., Hale, B.: There can be no compromise: The necessity of ratcheted authentication in secure messaging. *IACR Cryptol.* **2020**, 541 (2020). ePrint Arch
27. Esser, A., May, A., Verbel, J., Wen, W.: Partial key exposure attacks on bike, rainbow and ntru. *Cryptology ePrint Archive, Report 2022/259* (2022). <https://ia.cr/2022/259>
28. ESTI: Etsi ts 103 744 v1.1.1, cyber; quantum-safe hybrid key exchanges. Tech. rep., European Telecommunications Standards Institute (ETSI) (2020)
29. eVisit: The Ultimate HIPAA Guide: The Facts You Need to Know (2022). <https://evisit.com/resources/hipaa-guide/> [Accessed: 2022-03-29]
30. Faruk, M.J.H., Miner, P., Coughlan, R., Masum, M., Shahriar, H., Clincy, V., Cetinkaya, C.: Smart connected aircraft: Towards security, privacy, and ethical hacking. In: 2021 14th International Conference on Security of Information and Networks (SIN), vol. 1, pp. 1–5. IEEE (2021)
31. Federal Aviation Administration: Nextgen equip ads-b ins and outs (2021). [https://www.faa.gov/nextgen/equipadsb/capabilities/ins\\_outs/](https://www.faa.gov/nextgen/equipadsb/capabilities/ins_outs/) [Accessed: 2022-03-29]
32. Federal Office for Information Security: Migration zu post-quanten-kryptografie handlungsempfehlungen des bsi (german). Tech. rep., Bundesamt für Sicherheit in der Informationstechnik (BSI) (2020)
33. Feo, L.D., Jao, D., Plüt, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.* **8**(3), 209–247 (2014)
34. Frustaci, M., Pace, P., Aloï, G., Fortino, G.: Evaluating critical security issues of the iot world: Present and future challenges. *IEEE Internet Things J.* **5**(4), 2483–2495 (2017)
35. Fuchs, C.M., et al.: The evolution of avionics networks from ARINC 429 to AFDX. In: Innovative Internet Technologies and Mobile Communications (IITM), and Aerospace Networks (AN), vol. 65, pp. 1551–3203 (2012)
36. Gibney, E.: The quantum gold rush. *Nature* **574**(7776), 22–24 (2019)
37. Gidney, C., Ekerå, M.: How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum* **5**, (2021). <https://doi.org/10.22331/q-2021-04-15-433>
38. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: G.L. Miller (ed.) *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, Philadelphia, Pennsylvania, USA, May 22–24, 1996, pp. 212–219. ACM (1996)
39. Haggard, S., Lindsay, J.R.: North korea and the sony hack: Exporting instability through cyberspace. *Analysis from the East-West Center* (2015). <https://www.jstor.org/stable/resrep06456>
40. Hale, B., Van Bossuyt, D.L., Papakonstantinou, N., O'Halloran, B.: A zero-trust methodology for security of complex systems with machine learning components. In: *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, vol. 85376, p. V002T02A067. American Society of Mechanical Engineers (2021)
41. Harkins, D.: Dragonfly key exchange. Tech. rep., Internet Research Task Force (IRTF) (2015)
42. Hashemian, A., Arnholt, B.: Nuscale power module instrumentation. *Nucl. Plant J. (Online)* **36**(4), (2018)
43. Hassan, W.H., et al.: Current research on internet of things (iot) security: A survey. *Comput. Netw.* **148**, 283–294 (2019)
44. Huelsing, A., Butin, D., Gazdag, S., Rijneveld, J., A., M.: Mss: Extended hash-based signatures. Tech. rep., RFC 8391 (2018)
45. Huhnlein, D., Korte, U., Langer, L., Wiesmaier, A.: A comprehensive reference architecture for trustworthy long-term archiving of sensitive data. In: 2009 3rd International Conference on New Technologies, Mobility and Security, pp. 1–5. IEEE (2009)
46. Humboldt University Berlin SarWiki: WPA3 Dragonfly Handshake (2022). [https://sarwiki.informatik.hu-berlin.de/WPA3\\_Dragonfly\\_Handshake](https://sarwiki.informatik.hu-berlin.de/WPA3_Dragonfly_Handshake) [Accessed: 2022-03-29]
47. IDQ: Cerberis XG QKD system: quantum key distribution for enterprise, government and telco production environments (2022). <https://www.idquantique.com/quantum-safe-security/products/cerberis-xg-qkd-system/> [Accessed: 2022-03-29]

48. IEEE: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments (2010). IEEE Standard 802.11p
49. InfiniQuant: InfiniQuant (2022). <https://infiniquant.com/> [Accessed: 2022-03-29]
50. Information Security Oversight Office, N.A., Administration, R.: ISO Notice 2017-02: Clarification of Classification by Compilation. <https://www.archives.gov/files/isoo/notices/notice-2017-02.pdf> (2017). Accessed: 2022-03-27
51. Joux, A., Odlyzko, A., Pierrot, C.: The past, evolving present, and future of the discrete logarithm. In: *Open Problems in Mathematics and Computational Science*, pp. 5–36. Springer (2014)
52. Kadet, K.: Entrust. Entrust Helps Enterprises Prepare Now for Post Quantum Security Journey with New PQ Testing and Development Solutions (2022). <https://www.entrust.com/newsroom/press-releases/2022/entrust-helps-enterprises-prepare-now-for-post-quantum-security-journey> [Accessed: 2022-03-29]
53. Katz, J., Lindell, Y.: *Introduction to Modern Cryptography*. Chapman and Hall/CRC Press, London (2007)
54. Kelly, J.: A Preview of Bristlecone, Google’s New Quantum Processor. <https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html> (2018). Accessed: 2018-07-23
55. KETS Quantum: KETS (2022). <https://kets-quantum.com/> [Accessed: 2022-03-29]
56. Krishna, C.L., Murphy, R.R.: A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In: *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, pp. 194–199. IEEE (2017)
57. Lynch, C.: *Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust*. Routledge, New York (2013)
58. MacQuarrie, E.R., Simon, C., Simmons, S., Maine, E.: The emerging commercial landscape of quantum computing. *Nat. Rev. Phys.* **2**(11), 596–598 (2020)
59. MagiQ Tech: MagiQ (2022). <https://www.magiqtech.com/> [Accessed: 2022-03-29]
60. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of things (iot) security: Current status, challenges and prospective measures. In: *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336–341. IEEE (2015)
61. Mavroeidis, V., Vishi, K., Zych, M.D., Jøsang, A.: The impact of quantum computing on present cryptography. Preprint (2018). arXiv:1804.00200
62. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: *Handbook of Applied Cryptography*. CRC Press, London (2018)
63. Michele Mosca, J.M.: A methodology for quantum risk assessment (2017). <https://globalriskinstitute.org/publications/3423-2/> [Accessed: 2022-03-29]
64. Moir, I., Seabridge, A.: *Design and Development of Aircraft Systems*, vol. 67. Wiley, New York (2012)
65. Mosca, M.: Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Secur. Priv.* **16**(5), 38–41 (2018)
66. Moteff, J., Parfomak, P.: *Critical infrastructure and key assets: definition and identification*. Tech. rep., Library of Congress Washington DC Congressional Research Service (2004)
67. Motta, A.T., Capolungo, L., Chen, L.Q., Cinbiz, M.N., Daymond, M.R., Koss, D.A., Lacroix, E., Pastore, G., Simon, P.C.A., Tonks, M.R., et al.: Hydrogen in zirconium alloys: A review. *J. Nucl. Mater.* **518**, 440–460 (2019)
68. Mumtaz, M., Ping, L.: Forty years of attacks on the rsa cryptosystem: A brief survey. *J. Discrete Math. Sci. Cryptogr.* **22**(1), 9–29 (2019)
69. Murdoch, S.J., Drimer, S., Anderson, R.J., Bond, M.: Chip and PIN is broken. In: *31st IEEE Symposium on Security and Privacy, S&P 2010, 16–19 May 2010, Berkeley/Oakland, California, USA*, pp. 433–446. IEEE Computer Society (2010)
70. Mürer, N., Gräupl, T., Schmitt, C.: L-band Digital Aeronautical Communications System (LDACS). Internet-Draft draft-ietf-raw-ldacs-10, Internet Engineering Task Force (2022). Work in Progress

71. National Coordination Office for Space-Based Positioning, Navigation, and Timing: GPS.GOV: Official U.S. government information about the Global Positioning System (GPS) and related topics: Space Segment (2022). <https://www.gps.gov/systems/gps/space/> [Accessed: 2022-03-29]
72. Neuman, B.C., Ts'o, T.: Kerberos: An authentication service for computer networks. *IEEE Commun. Mag.* **32**(9), 33–38 (1994)
73. Papakonstantinou, N., Hale, B., Linnosmaa, J., Salonen, J., Van Bossuyt, D.L.: Model driven engineering for resilience of systems with black box and ai-based components. In: *Reliability and Maintainability Symposium* (2022)
74. Papakonstantinou, N., Van Bossuyt, D.L., Linnosmaa, J., Hale, B., O'Halloran, B.: A zero trust hybrid security and safety risk analysis method. *J. Comput. Inf. Sci. Eng.* **21**(5), 1–26 (2021)
75. Paquin, C., Stebila, D., Tamvada, G.: Benchmarking post-quantum cryptography in TLS. In: J. Ding, J. Tillich (eds.) *Post-Quantum Cryptography—11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings. Lecture Notes in Computer Science*, vol. 12100, pp. 72–91. Springer (2020)
76. Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al.: Advances in quantum cryptography. *Adv. Opt. Photon.* **12**(4), 1012–1236 (2020)
77. Pittaluga, M., Minder, M., Lucamarini, M., Sanzaro, M., Woodward, R.I., Li, M.J., Yuan, Z., Shields, A.J.: 600-km repeater-like quantum communications with dual-band stabilization. *Nat. Photon.* **15**(7), 530–535 (2021)
78. Post Quantum: Simple, secure, now (2022). <https://www.post-quantum.com/> [Accessed: 2022-03-29]
79. PQShield: Understanding the quantum threat, post-quantum cryptography and the upcoming NIST standards (2022). <https://pqshield.com/quantum-threat/> [Accessed: 2022-03-29]
80. Qabacus: Welcome to the Future Website of Qabacus Blockchain! (2022). <https://www.qabacus.com/> [Accessed: 2022-03-29]
81. Qaisec: Quantum encryption and AI (2022). <http://www.qaisec.eu/> [Accessed: 2022-03-29]
82. QBT: Quantum Blockchain Technologies (2022). <https://quantumblockchaintechnologies.co.uk/> [Accessed: 2022-03-29]
83. QRATE: Quantum Solutions (2022). <https://grate.online/> [Accessed: 2022-03-29]
84. Qrypt: Eternal Encryption (2022). <https://www.qrypt.com/> [Accessed: 2022-03-29]
85. Quantique, C.: Scalable IoT security from chip to cloud (2022). <https://www.cryptoqueantique.com/> [Accessed: 2022-03-29]
86. Quantum Dice: Securing a Connected Future (2022). <https://quantum-dice.com/> [Accessed: 2022-03-29]
87. Quantum Xchange: Delivering the Future of Encryption (2022). <https://quantumxc.com/> [Accessed: 2022-03-29]
88. QuBalt: Security Solutions for the Quantum Internet, Quantum Key Distribution Networks and Safety-Critical Systems (2022). <https://www.qubalt.de/> [Accessed: 2022-03-29]
89. QuSecure: Scalable Cybersecurity for the Post-Quantum Enterprise (2022). <https://www.qusecure.com/> [Accessed: 2022-03-29]
90. Räsänen, M., Mäkynen, H., Möttönen, M., Goetz, J.: Path to european quantum unicorns. *EPJ Quantum Technol.* **8**(1), 5 (2021)
91. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems (reprint). *Commun. ACM* **26**(1), 96–99 (1983)
92. Robling Denning, D.E.: *Cryptography and Data Security*. Addison-Wesley Longman Publishing Co., Boston (1982)
93. Sampigethaya, K., Poovendran, R., Shetty, S., Davis, T., Royalty, C.: Future e-enabled aircraft communications and security: The next 20 years and beyond. *Proc. IEEE* **99**(11), 2040–2055 (2011)
94. Shaikh, F., Rahouti, M., Ghani, N., Xiong, K., Bou-Harb, E., Haque, J.: A review of recent advances and security challenges in emerging e-enabled aircraft systems. *IEEE Access* **7**, 63164–63180 (2019)

95. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **41**(2), 303–332 (1999)
96. Sikeridis, D., Kampanakis, P., Devetsikiotis, M.: Post-quantum authentication in TLS 1.3: A performance study. In: 27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23–26, 2020. The Internet Society (2020)
97. Simmons, G.J.: Symmetric and asymmetric encryption. *ACM Comput. Surv. (CSUR)* **11**(4), 305–330 (1979)
98. Srivastava, R., Choi, I., Cook, T., Team, N.U.E.: The Commercial Prospects for Quantum Computing. Networked Quantum Information Technologies (2016)
99. Support, D.: Apps and Keys (2022). <https://support.docusign.com/guides/ndse-admin-guide-api-and-keys> [Accessed: 2022-03-29]
100. Van Meter, R.: Security of quantum repeater network operation. Tech. rep., Keio University Fujsawa Japan (2016)
101. Van Tilborg, H.C., Jajodia, S.: *Encyclopedia of Cryptography and Security*. Springer Science & Business Media, New York (2014)
102. Vanhoef, M., Ronen, E.: DRAGONBLOOD: Analysing WPA3’s Dragonfly Handshake (2022). <https://wpa3.mathyvanhoef.com/> [Accessed: 2022-03-29]
103. VeriQloud: Quantum Cybersecurity Unlocked (2022). <https://veriqcloud.com/> [Accessed: 2022-03-29]
104. Windows App Development: Microsoft Kerberos (2022). <https://docs.microsoft.com/en-us/windows/win32/secauthn/microsoft-kerberos> Accessed: 2022-03-29]
105. Yanez, J., Kuznetsov, M., Souto-Iglesias, A.: An analysis of the hydrogen explosion in the fukushima-daiichi accident. *Int. J. Hydrogen Energy* **40**(25), 8261–8280 (2015)
106. Yun, A., Shi, C., Kim, Y.: On protecting integrity and confidentiality of cryptographic file system for outsourced storage. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, pp. 67–76 (2009)
107. Zetter, K.: *Feds Say That Banned Researcher Commandeered a Plane* (2015)
108. Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K., Shieh, S.: Iot security: ongoing challenges and research opportunities. In: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234. IEEE (2014)

# On the Way to Coastal Community Resilience Under Tsunami Threat



Mark Klyachko, Andrey Zaytsev, Tatiana Talipova, and Efim Pelinovsky

## 1 Introduction

The sea and ocean coasts have always been and remain particularly attractive for human development despite the fact that they are subject to the greatest natural threats. At the same time, the most terrible marine threat is the tsunami. In order to accumulate a sufficiently complete knowledge of the tsunami nature and to understand better how to respond to this threat and how to warn the coastal community about tsunamis in advance, it took scientists many centuries to establish the fact that the main tsunami source is quite powerful (with the magnitude of  $M > 7$ ) earthquakes; therefore, tsunamis should be expected primarily on the Pacific Rim coast where 80% of the earth seismic energy is released.

In 1988, at the initiative of the President of the National Science Foundation (USA) Prof. Thomas Press proposed and then adopted the UN Tokyo Declaration

---

M. Klyachko

Regional Alliance for Disaster Analysis & Reduction, NPO, Saint Petersburg, Russia

A. Zaytsev

Special Research Bureau for Automation of Marine Researches, Far Eastern Branch of Russian Academy of Sciences, Yuzhno-Sakhalinsk, Russia

e-mail: [aizaytsev@mail.ru](mailto:aizaytsev@mail.ru)

T. Talipova

Institute of Applied Physics, Nizhny Novgorod, Russia

V.I. Il'ichev Pacific Oceanological Institute, Vladivostok, Russia

E. Pelinovsky (✉)

Institute of Applied Physics, Nizhny Novgorod, Russia

V.I. Il'ichev Pacific Oceanological Institute, Vladivostok, Russia

National Research University - Higher School of Economics, Moscow, Russia

e-mail: [pelinovsky@appl.sci-nnov.ru](mailto:pelinovsky@appl.sci-nnov.ru)

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023

K. P. Balomenos et al. (eds.), *Handbook for Management of Threats*, Springer

Optimization and Its Applications 205,

[https://doi.org/10.1007/978-3-031-39542-0\\_8](https://doi.org/10.1007/978-3-031-39542-0_8)

on Disaster Reduction (IDNDR); it recognized that while natural hazards such as earthquakes and tsunamis are not yet manageable, humanity can and should if though not prevent but at least reduce their undesirable consequences.

The importance of tsunami safety for Russia is due to the large length of its seacoasts. We will list here the Russian sea coasts in order of decreasing tsunami threat level: the Kamchatka–Kuril region in the northwest of the Pacific Rim, the Black Sea coast, the Caspian Sea coast (actually the world’s largest lake), the Azov Sea coast, and, finally, Lake Baikal, which is located in a very high seismicity zone. For example, due to the 1892 Tsagan earthquake, the coastal territory collapsed forming a bay with the same name Sinkhole and causing tsunami waves (seiches) up to 3.5 m high. The highest tsunami heights in Russian history were noted [64] on the coast of the Kamchatka Peninsula, located in the subduction zone not far from the Kamchatka–Kuril deep-sea trench. The Okhotsk Sea coast of Kamchatka is subject to high tides, the height of which increases to the north and reaches 13 m in Penzhina Bay. In addition, at the bottom of the Okhotsk Sea there are several underwater volcanoes, the possible activity of which is also fraught with dangerous tsunamis. There are also several data on tsunamis in the country’s inland waters mainly caused by landslides [10]. Let us especially note the wave in the Bureya River in December 2018, when the splash height was 90 m [46]. The development of existing coastal cities and tourist complexes, civilization, and economic development of new sea coasts, seaport construction and reconstruction, shipbuilding and fish processing facilities, and gas and oil production in the sea makes the tsunami protection problem of the Russian Federation sea coasts very important and urgent.

The purpose of the present paper is to describe orderly the ways, mechanisms, and tool box recommended to reduce tsunami disasters ensuring sustainable sea coast safety on the examples of research carried out in Russia based on Set of Rules 292.1325800.2017 “Buildings and structures on tsunami hazardous areas. Regulations of design” (further Set of Rules 292) and supporting these Set of Rules 292 manuals [48, 49]. At the same time, for the convenience of computer processing in GIS and for the future development of RObot Interaction LANguage (ROILA), a large number of associative abbreviations were used; in the present paper, they are written together with their concept decoding, with the exception of regularly repeated abbreviations, the concept of which is given in paragraph 7 “Nomenclature.”

## **2 The Software Block Approach to Ensuring the Sea Coast Sustainable Safety**

### ***2.1 The Typical Program and the Block Diagram of Preventive Security of Urban Areas Prone to Natural Hazards***

The Kamchatka Peninsula, the eastern region of the Russian Federation, located in the northwestern part of the Pacific Rim, has extremely diverse ground conditions and is subject to the country’s most dangerous volcanic eruptions, earthquakes,



hurricanes, and tsunamis. Thus, in connection with it, since the late 1960s this territory has become an experimental site for engineering seismometric observations on residential buildings of various design solutions and for testing the seismic resistance of buildings with various types of seismic isolation.

When solving the problem of population safety and the territories prone to natural hazards, which mankind is not yet able to rule, the R&D Center on Earthquake Engineering and Natural Disaster Reduction (CENDR, Russia) developed (1986–1992) the program “PREventive Sustainable Safety” (PRESS) suitable to protect the diverse socioeconomic urbanization systems (SESURB) subject to any unmanaged hazardous natural impacts [26].

The standard “PREventive Sustainable Safety” (PRESS) program consists of two parts:

$$\text{PRESS} = \text{PRANA} + \text{PRIMA}, \tag{1}$$

where the PRANA subprogram is the Program Risk ANALysis, while the PRIMA subprogram is the Program RIsk Management.

The complexity of the PRESS lies in the mandatory consideration of additional probable tsunami triggers (underwater and coastal landslides, landslides, etc.), secondary natural and anthropogenic impacts, and simultaneous/associated disasters, for example, epidemiological or of climatic origin. With regard to the tsunami protection problem, the implementation of the PRANA and PRIMA subprograms should be carried out by sequentially solving tasks combined into target blocks, as indicated in the flowchart in Fig. 1 [41].

To solve the task of ensuring the seismic safety SESURB around Avacha Bay (Kamchatka, Russia), set by Decree No. 2359-r of the Russian Government dated November 21, 1986, the PRESS-integrated program was turned into a locally targeted integrated preventive seismic safety program with the same abbreviation

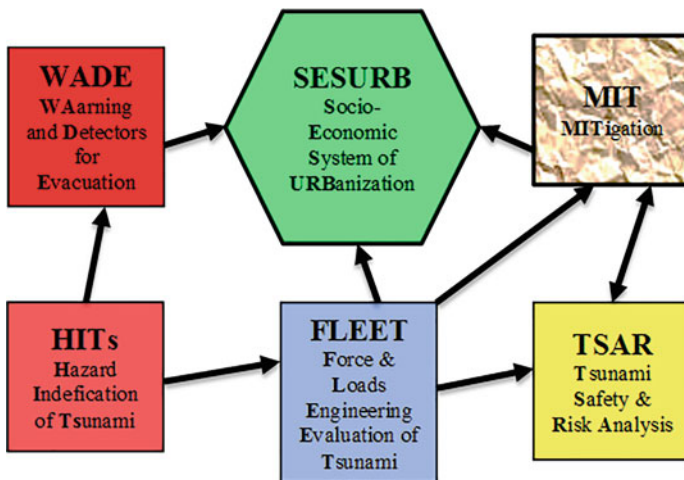


Fig. 1 Block diagram of the PRESS implementation on tsunami-prone coasts



(in Russia it was called later “Seismoprotection”). In the last decade of the twentieth century, while the tasks of seismic safety were being solved, the tsunami problem in the Avacha Bay water area was considered to be a secondary hazard; but, unfortunately, the issues of structure tsunami protection were not solved, among them the lack of the engineering approach and relevant building codes including. It should be taken into account that (i) about 80% of tsunamis are seismogenic, which is why our greatest focus is laid on tsunamis caused by earthquakes and (ii) the greatest disasters on sea coasts occur as a result of the cumulative impact of earthquakes close to them and the subsequent seismogenic tsunamis. Today, we can and must return to a comprehensive analysis and disaster management in a generalized standard setting, combining the impact of earthquakes and tsunamis to various degrees and taking into account possible secondary and associated disasters.

## 2.2 Database for Tsunami Risk Analysis

The tsunami risk management target is the THA (tsunami hazardous area), which is planned for future development/building construction or that has already been urbanized. The THA includes water areas adjacent to the shore with a depth of up to 50 m and the coastal area limited by the flood line based on the tsunami microzoning results (DEM/TMZ). A variety of materials necessary to analyze the complex tsunami risk on the sea coasts are a kind of AMFORA (Applied Material for FORMula of Risk Analysis) that is replenished from two main sources:

- Basic information-analytical data/Informatics-Analytics DataBASE (DIABASE), directly related to the considered tsunami-prone area/the THA and received in this area.
- The data obtained outside the THA under consideration, mainly from the survey results of the disaster tsunami consequences and the rehabilitation experience and recovery of areas affected by natural disasters, additionally selected from the Bank of Knowledge and Experience/BANK of KNOWledge, Testing and Experience in the Safety (BANKNOTEs).

Thus,

$$\text{AMFORA} = \text{DIABASE} + \text{BANKNOTEs} \quad (2)$$

The DIABASE database for the THA is represented in GIS and consists of bathymetric and topographic maps, geotechnical data (including the landslide hazard), the bottom sediment characteristics, tides, surge/wind waves, a building map, and the peculiarities of the existing urbanized area, which is produced, for example, by using the ArcGIS Desktop PC. The DIABASE of a specific THA is constantly updated based on the THA certification results in terms of vulnerability assessments of the population, in terms of planning, design, and functional building vulnerability (including hard-to-evacuate, potentially dangerous facilities, life sup-

port facilities, networks/key building, and critical facilities) to a probable tsunami and to the triggers that called it. The VULCAN (VULnerability City ANalysis) toolkit is used to assess the building vulnerability and the one connected with the population of the city. It also describes the educational, cultural, and psychophysical characteristics of the THA population, their disaster experience, the level of medical care, and other characteristics and factors influencing the generalized vulnerability assessments of the population to earthquakes and tsunamis, readiness for evacuation, the panic likelihood, seismophobia, etc. [39]. Instructions on the layout and content of the DIABASE (Informatics-Analytics DataBASE) are given in [48]. Such a database for the tsunami risk analysis was developed by us for the first time for the city of Petropavlovsk–Kamchatsky in pursuance of the Decrees of the Russian Government dated December 5, 1989, No. 1090 and February 27, 1990, No. 75 on accelerating the solution to the problem of ensuring the urbanized area safety around Avacha Bay at a predicted destructive earthquake. The PRANA subprogram uses various combinations of the deterministic approach typical for the DIABASE and the probabilistic analysis, which is impossible to do without in the field of new knowledge. That is why one should be very careful when creating and using the data from the BANKNOTES (BANK of KNOWledge, Testing and Experience in the Safety). Unfortunately, many urbanized coasts do not have their own experience of disasters from earthquakes and even more so from tsunamis. Therefore, it is really of utmost importance to study carefully and comprehensively all tsunami disasters, to search for and find similar objects, or identical SIB (SImilar Buildings) buildings, whose vulnerability to tsunamis is reliable, and to single out the BAOBAB (Basic OBjects for Analysis of the Built-up) from them equipped with engineering observation stations. For reliable estimates of probable tsunami disasters at the THA with insufficient own disaster experience, the combined mathematical method MELESA (Method of Expert-Logical Estimations and System Analysis) is used; it is built based on the theory of “fuzzy sets” and blurred images. An orderly approach to the formation of the AMFORA database for the urbanized areas with insufficient own disaster experience was finally formed in CENDR by 1993 [29]; the formation of the minimum list of the SIB analog objects was completed in 1995 by using the consequences of domestic earthquakes in Ashgabat (1948), Petropavlovsk–Kamchatsky (1952, 1971), Tashkent (1966), Gazli (1976), Spitak (1988), Sakhalin region (1994, 1995) and abroad in Italy (Artegna, 1976, and in 1980 Campania–Basilicata, Balvano, San Angelo Dei Lombardi), Montenegro (Yugoslavia 1979), Asman (Algeria 1980), Mexico City (1985), Iran (Manjil, 1990), and Turkey (Erzincan, 1992). The resulting set of the SIBs is sufficient for a reliable probable seismic risk analysis. At the 11th European Conference for earthquake engineering (Paris, 1998), the Working Group “Seismic risk. Vulnerability. Disaster scenarios” with the co-chairmen M. Dolce (Italy) and M. Klyachko (Russia) was organized.

### 3 Methods and Mechanisms/the Toolbox for the Tsunami Risk Analysis and Management

Within the framework of the present paper, we restrict ourselves to listing below the main methods and tools used in PRANA and PRIMA making the minimum necessary comments. At the same time, we will consider the worst case of the multifactorial disaster on a conditional coastal urbanized territory subject to a local tsunami with a closely located seismic trigger and with the additional tsunami amplifying factors (e.g., underwater and coastal landslides similar to September 28, 2018, on the Sulawesi Island, Indonesia) [65, 66]. Disaster mitigation tools should be subdivided into research, engineering, regulatory, educational, and special regulation methods. The fact that these areas of activity are carried out by specialists of various profiles and officials shows that coordination of this complex work is required in order to gain the effective result.

#### 3.1 *The Tsunami Warning System*

At present, the Tsunami Warning System is already operating in several regions of the world (the Pacific and Indian Oceans, and the Mediterranean Sea), issuing an operational tsunami forecast immediately after the  $M > 7$  earthquake. It should be taken into account that the Tsunami Warning System (TWS) may fail to work and maybe late with an alarm. Moreover, repeated false alarms of the Tsunami Warning System prevent people from responding to real danger in a timely and correct manner. Even the most advanced TWS in Japan could not prevent the death of more than 14,000 people from the tsunami on March 11, 2011, if counting only drowned people. Much work is being done to improve the efficiency of the TWS by increasing the number of tsunami buoys (DART type), the submarine cable used, the satellite data, and methods used to calculate tsunami characteristics, the presentation of which is beyond the scope of this paper.

#### 3.2 *Tsunami Hazard Assessment*

For a long-term forecast of tsunami characteristics and their impact on coastal infrastructure, it is first necessary to estimate the prognostic wave height (tsunami hazard). It is associated with the probability  $P$  that at least one tsunami with a run-up height exceeding the value  $h$ , calculated in the framework of the Poisson law for rare events, will occur in the given place during time  $t$

$$P(h, t) = 1 - \exp[-\varphi(h)t], \quad (3)$$

where the average tsunami frequency  $\varphi(h)$  with a run-up height exceeding the level  $h$  is called the recurrence function. This function is determined based on historical tsunami data (if there are enough such data) and/or prognostic tsunami calculations. Set of Rules 292 for the Russian Far East coast now uses a recurrence function based on historical data. It is well approximated by the exponent for  $h > 0.5$  m:

$$\phi(h) = f \exp(-h/h^*), \quad (4)$$

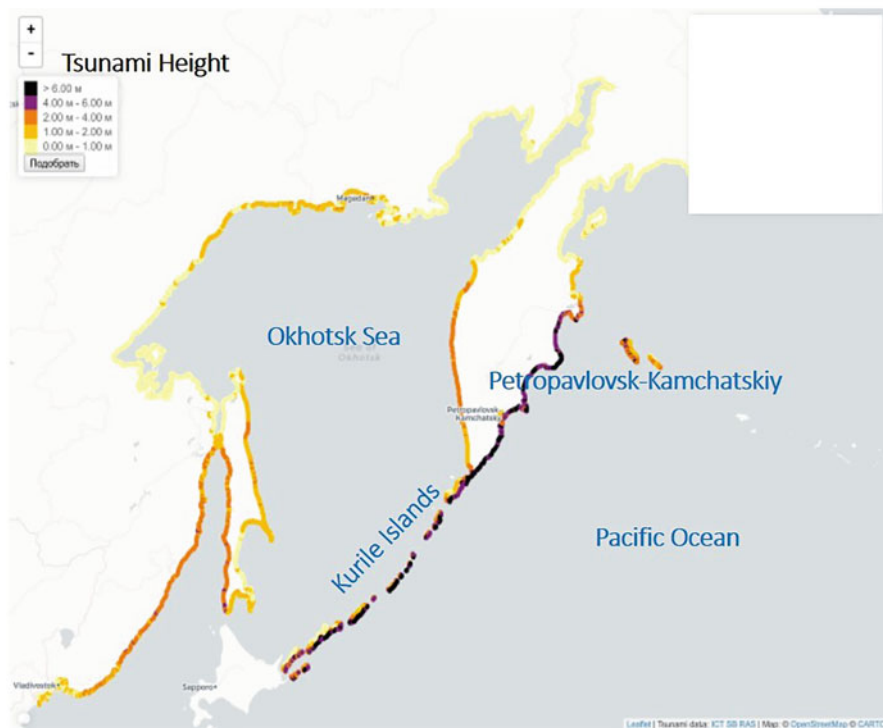
where  $f$  is the frequency of strong tsunami appearance (regional parameter) and  $h^*$  is the characteristic tsunami height (local parameter). The tsunami hazard can be presented in cartographic and tabular form. For example, in the design code Set of Rules 292 tsunami zoning is represented on maps in three scale ranges: M1:5000000–M1:1000000; M1:1000000–M1:25000; M1:25000; and larger, depending on the detail and the number of parameters taken into account.

$$h_{50} = h^* \cdot \ln(50f); \quad (5)$$

$$h_{100} = h^* \cdot \ln(100f). \quad (6)$$

To assess the tsunami resistance of the increased responsibility objects, Set of Rules 292 uses the run-up level  $h_{50;0,1}$ , which approximately corresponds to an average frequency of once every 500 years; in the IAEA standards, when designing nuclear power plants, the maximum tsunami level is taken once every 10,000 years. Such values cannot be obtained from the analysis of only historical tsunamis, and here, the PTHA (Probabilistic Tsunami Hazard Assessment) method is used, in which the historical tsunami data are supplemented with the predictive tsunami data from possible earthquakes; see, for example [4]. In this method, the source is a synthetic catalog of earthquakes that are possible over a period of 100 thousand years, based on the available data extrapolation on the geological structure of the earth and seismic activity. Then, possible tsunamis caused by such events are calculated with estimates of all available uncertainties. As a result, it is possible to give probabilistic characteristics of tsunami heights on the coast necessary to assess the risks associated with the tsunami. Such studies have already been carried out for the US Pacific coast [14], the Mediterranean Sea basin [3], and the Russian Far East coast [17]. An example of calculating the tsunami hazard map of the Far East coast of Russia with the probability of exceeding the given height of 10% for a period of 50 years, which is equivalent to the tsunami with such a height once every 475 years, is shown in Fig. 2 taken from [17].

Let us note that tsunami hazard maps are built based on a huge number of scenarios, which is very costly. Therefore, the tsunami heights in these maps are calculated near the coastline (at a depth of several meters) and with a certain average along the coast. These figures are actually the starting points for tsunami microzoning, when the size of the coastal flood zone, the water flow depth, and



**Fig. 2** Tsunami hazard map of the Far East coast of Russia with the probability of exceeding the given height of 10% for the period of 50 years

speed on the coast are estimated [13]. The result is a tsunami set of the HAZard Scenario (HAZS) for the possible events with the given probability.

When carrying out microzoning, the flood zone parameters of the coast are specified, taking into account the differences between the considered coast and the “standard coast” adopted in Set of Rules 292, as well as taking into account the THA development. When these tasks are performed, the weak point is the need to have detailed bathymetric maps and the coastal zone topography with scale of up to several meters. In numerical calculations of tsunami scenarios, the nonlinear shallow water theory and its dispersion generalizations are usually used. One of the popular computing systems used to solve these problems is the NAMI-DANCE, developed in collaboration with Turkish and Russian specialists [65, 66]. Figure 3 taken from [2] shows an example of calculating the coast flooding of the port of Haydarpasa, located in the Sea of Marmara near the metropolis of Istanbul (Turkey), by a possible catastrophic tsunami. The wave height in this place can exceed 6 m, and the waves arrive at the port in a few minutes. The maximum port flooding will occur 20 min after the tsunami occurrence. The water flow will move at a high speed (about 5 m/s) and cause a lot of damage in the port. It is worth noting that



**Fig. 3** Maximum flooding zone by tsunami waves of the port of Haydarpasa

all calculations are made taking into account the onshore and offshore structures; therefore, it becomes possible to calculate the force action on these objects.

In order to characterize the destructive tsunami power under the action of the water flow on the coast on average, various intensity scales are used; see, for example [54]. In our research and Set of Rules 292, we use the following scale, presented in Table 1.

In our research and practice, we use the categories of structural building vulnerability in accordance with Note 5 to the tsunami intensity scale (Table 1).

Fragility curves with classification of various structures are now being widely used; see, for example [53, 56, 62]. However, everything related to the term “fragility” seems to have a very limited scope, since fragility is only inherent in stone structures, large-block concrete houses, and poorly designed reinforced concrete frame buildings. Building structures made of wood, metal structures, modern nanostructured concrete, and other building materials with high ductility are not subject to brittle damage and destruction. What is more, a higher ductility has tall hotel buildings common on seashores, equipped with seismic isolation systems and/or dampers to dampen dynamic vibrations.

### ***3.3 Tsunami Engineering Survey and Physical Modeling***

Engineers obtain the most valuable knowledge about the tsunami interaction with buildings and structures because of examining the tsunami consequences. The

engineering consequences of the December 27, 2004, tsunami in the Indian Ocean are best studied [9, 51], and the 2010 tsunami surveys in Chile were also interesting and useful [50, 55].

A recent survey of the consequences of the tsunami caused by an  $M = 7.0$  earthquake in the Aegean Sea showed that a seismogenic weak tsunami was in

**Table 1** Tsunami intensity scale

Intensity $I_{ts}$		Typical effects/consequences observed on the coast and adjacent waters
Qualitative characteristic (term) strength, consequences	Quantitative characteristics, points	
Imperceptible	0	( $\alpha$ ) The run-up height does not exceed 0.5 m, which is imperceptible and is noted only by tide gauges
Extremely weak/perceptible	I	( $\alpha$ ) The run-up height is 0.5–1 m, which is noticed by a few and recorded by tide gauges ( $\gamma$ ) Certain offshore structures of vulnerability category (f) and certain coastal structures of vulnerability category (vh) receive damage of degree 1
Weak	II	( $\alpha$ ) The run-up height is 1–2 m, which is observed by everyone ( $\beta$ ) Flat coasts are flooded; lightships are thrown ashore ( $\gamma$ ) Many coastal structures of vulnerability category (f) receive degree damage 1, some damage – degree 2; coastal structures of vulnerability category other than (f) and most coastal structures are not damaged
Moderate/damaging	III	( $\alpha$ ) The run-up height is 2–4 m ( $\beta$ ) Lightships are thrown or swept away; the shores are littered with rubble and litter ( $\gamma$ ) Many buildings and structures of vulnerability categories (f) and (vh) have degree damage 3. Some of them have degree damage 4. Many buildings of vulnerability category (mh) have degree damage 2, and some of them have degree damage degree 3. Some buildings of category (m) have degree damage 2. Some buildings of vulnerability category (lm) have damaged degree 1

(continued)

**Table 1** (continued)

Intensity $I_{ts}$		Typical effects/consequences observed on the coast and adjacent waters
Qualitative characteristic (term) strength, consequences	Quantitative characteristics, points	
Strong/ strongly damaging	IV	( $\alpha$ ) The run-up height is 4–8m ( $\beta$ ) Large ships are damaged and/or stranded; there is heavy soil erosion from fields. In the absence or failure of the SPM, individual victims ( $\gamma$ ) Most buildings in the vulnerability categories (f) and (vh) have damaged levels 4 and 5. Many buildings in the vulnerability category (h) and some vulnerability categories (mh) have damaged up to degree 4. Some buildings in the vulnerability category (m) may be partially destroyed
Very strong/damaging	V	( $\alpha$ ) The run-up height is 8–16 m ( $\beta$ ) The entire flooded area is covered with debris. Many people are dying despite the SOC, sometimes there is panic ( $\gamma$ ) Many buildings of vulnerability category (mh) have damage up to degree 4
Catastrophic/damaging	VI	( $\alpha$ ) The run-up height is greater than 16 m ( $\beta$ ) Complete devastation of coastal territories along the front and in depth. A large number of victims, despite the SOC. Mass panic ( $\gamma$ ) Most buildings of vulnerability categories (h) and (mh) and some vulnerability categories (lm) are destroyed

Notes

1. In this table, the following designations are used: ( $\alpha$ ) – effects observed in the coastal marine area; ( $\beta$ ) – effects observed on the coast; ( $\gamma$ ) – effects observed on building structures
2. The tsunami run-up height is determined at the shoreline of the undeveloped standard coast
3. The damage degree of buildings under the tsunami influence is graduated from 0 (absence) to 5 (collapse) similar to those adopted in the earthquake-resistant construction
4. As an enlarged territorial tsunami characteristic, the intensity  $I_{ts}$  is taken, corresponding to the rounded run-up height value with the wave speed at the waterfront of 10 km per hour
5. The category of structural vulnerability of the coastal and near-the-coast buildings and structures is taken according to the classification [28, 31] or according to the European Macroseismic Scale (EMS-98)



places amplified by underwater landslides [63]. On the Turkish coast in small bays with narrow entrances, the tsunami was much stronger, and the impacts along these coasts were more serious: The maximum tsunami height of 2.3 m (with a flow depth of 1.4 m) was recorded in the Kaleici area in Sygachik; additionally, the tsunami intensity increased up to 3.8 m in places of numerous streams flowing into bays [11]. The tsunami flow traveled far along the streets of Izmir, and the flow velocity was obviously very high, as a result of which in insufficiently protected buildings the impact of the tsunami caused suffusion or liquefaction of the foundations' soil base, which, consequently, led to heeling, precipitation, and damage to these buildings. The lesson of the Aegean tsunami is that even a small tsunami can cause a big disaster, as "all disaster lessons are important in mitigating future disasters."

However, since disasters caused by tsunamis are fortunately very rare, the required knowledge is not sufficient. This deficiency is made up for by physical modeling, which, being an integral part of the FLEET block, makes it possible to obtain the most reliable knowledge about the formation of tsunami in real THA, the effectiveness of protective engineering structures (breakwaters, barrier structures), and the dynamic tsunami interaction with floating, offshore, and onshore facilities (taking into account vortex processes, the flow around, etc.) [5, 23, 24, 42, 43]. The performed work on experimental physical modeling makes it possible to supplement Set of Rules 292 with a section on the calculation and design of floating structures, which is planned to be completed in the near future when updating Set of Rules 292.

When examining the tsunami consequences, it is necessary to pay attention to the real readiness of the population for this disaster and the dependence of human losses and suffering on the level of this readiness. Education and training of the population for tsunami disaster preparedness play an important role in tsunami mitigation. In this direction of disaster management, we will note:

- When developing leaflets for the population, cultural, mental, age, psychophysical, housing, and other characteristics of the population should be taken into account, avoiding simple duplication of global standard recommendations.
- Advance preparation of a family action plan (in emergency situations) and an emergency kit.
- Advance knowledge of the procedure, routes, and final evacuation place, including the vertical evacuation.
- During the training, it is especially important to consolidate the methods and techniques of response by numerous repetitions to bring the reaction to automatism.
- Minimal knowledge and skills to provide primary health care.

All the items mentioned above are important in order to prevent panic (before and during the disaster) and long-term anxiety syndromes (including insomnia), to counteract various phobias (before the disaster) and shock situations (during the disaster), and to prevent or reduce cases of unreasonable injuries, pregnancy termination, and chronic diseases exacerbation (usually cardiological) [27, 35, 39, 67] as observed for the cause called "seismophobia" after the 1971 earthquake in Petropavlovsk–Kamchatsky, Russia. In this regard, not only the delayed TWS alert

can increase the disaster size, but also the frequent erroneous tsunami warnings lead to an undesirable inhibition of people's response to the expected tsunami; that is, both situations are harmful.

Popular tsunami books and brochures published by the International Tsunami Center in various languages play an important role. In Russia, special leaflets are published regularly for the population of Sakhalin, the Kuril Islands, and Kamchatka (although not all the issues raised above are reflected in them). Knowledge of basic information about the tsunami helped to avoid casualties on Kunashir Island (the Kuril Islands) during the 1994 Shikotan tsunami, when the warning system was broken and several people who knew about the tsunami organized the population retreat from the coast [19].

### ***3.4 Tsunami Risk Analysis and Management Through the Tsunami Design Code***

The concept of tsunami safety includes principled approaches, special conditions, and agreements [60]. Among them, in the first place is the main item stated in the International Decade for Natural Disaster Reduction, which says that engineers can and should manage disaster risk, reducing the vulnerability of buildings and the population of urban areas. The following items (statements) are also important in the concept: i) It is technically impossible and economically inexpedient to get fully protected against a tsunami; ii) the main objective of tsunami protection is to minimize the risk associated with the people's life and health, while the acceptable risk of material damage is determined by the owner.

The desired goal is the sustainable tsunami safety THA that is solved in the process of seacoast urbanization, implementing a block program approach (Sect. 2) through the development of regulatory documents (codes, guidelines, methodical manuals, recommendations, etc.) for the development and construction building development of these THA. Typical problems, tasks, and ways to solve them to improve the coastal community resilience are briefly discussed here using the example of the Russian tsunami design code [60], developed in 2016 by the Association "RADAR" in pursuance of the order of the Russian Government dated September 28, 2015, No. DK-P9-6620\* and approved by the order of the Ministry of Construction, Housing and Communal Services dated June 23, 2017, No. 915/pr.

Set of Rules 292, Manual 3 defines the tsunami loads and impacts on building structures and considers their structural vulnerability assessment, tsunami resistance, and damage, all that is carried out taking into account hydrodynamic loads, weighing forces, suffusion, soil base liquefaction, and other related and secondary influences. At the same time, special attention is paid to critical infrastructure (facilities and life support networks) and key facilities (difficult-to-evacuate buildings, buildings with vertical evacuation, and potentially dangerous objects). The option

of availability and timely TWS operation is considered, as well as the option when the TWS is absent or does not work in a timely manner.

Chapters “[Risk Assessment and Identification Methodology for the Defense Industry in Times of Crisis: Decision Making](#)”, “[Quantum Computers: The Need for a New Cryptographic Strategy](#)”, “[On the Way to Coastal Community Resilience Under Tsunami Threat](#)”, and the Set of Rules 292 deal with the problems, the consistent solution of which makes it possible to determine the loads and calculate the tsunami resistance of existing and designed buildings and structures, both in the water area and on the coastal part of the THA. In particular, Set of Rules 292 and [49] provide guidance on assessing the run-up of unbroken and broken (bore) waves on the shore and then the impact of these waves on non-streamlined, streamlined, and through marine HTS. The stages of design, operation, and monitoring of the technical condition of offshore hydraulic structures are well supported by building codes, which include calculations of these hydraulic structures for the impact of long wind waves. The Set of Rules 292 is entirely devoted to the calculation and design of tsunami-resistant coastal structures. To do this, their dynamic interaction with the bore was considered and the loading analysis was performed in the impact stage and in the stage of quasi-stationary flow; see also the original paper [57]. The increased duration in the drill pressure on the frontal face of the structure with some fundamental oscillation period is taken into account using the dynamic coefficient  $K_{dyn}$ , the standard value of which is taken according to a special schedule and does not exceed  $K_{dyn} = 2$ . Considering the stage of quasi-stationary flow around, we gave the formulas to determine the loads from bore run-up on impermeable and poorly permeable coastal objects of various shapes at different ratios of the structure size (width  $B$  and height  $H$ ) and the water flow depth  $d$ . It is accepted that the deformation of the flow-free surface can be neglected at  $B < 0.2d$  or  $H < 0.5d$ . Set of Rules 292 contains a large number of formulas, tables, and figures necessary and sufficient to determine the loads on almost any coastal facility.

Below, we will note some of the general provisions specified in Set of Rules 292. Tsunami building and structure resistance are ensured by the following:

- Facility location outside the THA and/or in the tsunami-protected areas.
- Space planning solutions that allow achieving maximum streamlining and the necessary, adjustable permeability of marine hydraulic structures, and the lower floors of coastal buildings for the tsunami flow.
- Strength and structure stability as a whole, individual load-bearing structures and non-bearing elements.
- Non-design, constructive measures, the choice of building materials that increase the structural strength and structure stability, and ensure maximum structure streamlining by tsunami flows.
- Progressive collapse prevention (PROCOL).
- With the help of engineering protection, including dams, reinforced concrete barriers, and barriers with a height exceeding the local calculated vertical splash of at least 25 cm, breakwaters, and other protective and bank protection structures.

- Measures to prevent large objects (vessels, cars) and debris from entering the tsunami stream.

The tsunami impact calculation is made according to the first (for strength) and in the specified [15, 16, 52] for the second limit state (for stability). At the same time, the tsunami resistance calculation according to the first limit state is mandatory for all objects, and the calculation according to the second limit state should be carried out for critical, key, and potentially dangerous objects. The calculation results must meet the relevant reliability requirements to the extent that the customer's requirements for maintaining the functional structure suitability are met, corresponding to the operable or, in extreme cases, limited operable structure state. These calculations should be made taking into account the interaction in the structure–soil system [36]. In this case, it is necessary to pay special attention to the design situations associated with structure violations and soil properties of the structure foundations due to erosion, soil liquefaction, and other negative processes caused by the tsunami wave run-up and run-back.

Set of Rules 292 specifies several criteria that depend on the structural damage degree corresponding to various allowable limit parameters. For example, the destruction or damage of non-structural elements (partitions, etc.) may cause the loss of the required operational suitability of the structure for evacuation. In relation to the specific building construction, the allowable material damage parameters are presented in terms of economic vulnerability. These parameters are included in the design task. Tsunami impact calculation is not mandatory for all buildings and structures located on the THA. The building owner has the right to assess the material damage that may be caused to this building in the tsunami event and to determine the allowable amount of such damage, if they wish to cooperate with the insurance company.

In Set of Rules 292, it is recommended to consider all structures subject to calculation, including tsunami protection, making their constructive calculation only for the operational period. In accordance with the customer's decision (e.g., for class I offshore HTS), it is allowed to make calculations for loads that take into account tsunamis for the construction period and the repair case. Three consecutive tsunami waves are taken as the most adverse effect of a tsunami. In the case of nearby tsunamis, its impact on structures is considered secondary, following the seismic one. At the THA, where nearby tsunamis are likely, the complex event earthquake with aftershocks → several tsunami run-ups and tsunami run-downs, with the soil erosion of the structure base, is considered several emergency design situations at different times, each of which has only one special load. The parameters of the design situation due to suffusion and soil liquefaction are recommended to be determined for different structure types, taking into account local conditions based on the results of physical modeling, which is mandatory for high-critical structures. Basic books for the analysis of potential soil liquefaction under the earthquake and tsunami influence are [18, 21, 59]. Auxiliary materials to assess the stability of soil subjected to hydrodynamic action are given in Annex B of [61]. A special section of Set of Rules 292 describes the geotechnical requirements and rules to be taken

into account in the calculation and design of the bases and foundations of building structures located on the THA. For through-type structures (flyovers, bridges, and bridge-type berths), it is necessary to consider the vertical impact load from the splash on the topsides. When calculating the tsunami resistance of structures located on the THA with seismogenic tsunamis, these structures should be considered with some initial predetermined degree of seismic damage. In this case, the degree of initial seismic damage can be determined based on the structural vulnerability class of the structure under consideration and the intensity of the tsunamigenic earthquake using EMS-98.

Of the transport structures, the most vulnerable to the tsunami effects are bridges across non-navigable rivers flowing into the sea, as well as bridges located on highways along the coast. Many bridges connecting the banks of small rivers collapsed, for example, during the tsunami on March 11, 2011, in Japan. Calculation and design requirements for the bridge supports and superstructures are set out in a special section of Set of Rules 292.

The worst design situation on small rivers is the heap on the bridge supports of the tsunami rolling into the sea, enhanced by the flow of river water containing ice. As for the designed bridge span, its bottom should be located at least 0.5 m above the maximum ice flow level, since in most cases it is impossible to prevent the bridge drop-down or the span destruction under such loads by any practical measures. Depending on the responsibility of the operated bridge and the specific design situation, it may be appropriate to install special local enclosing structures in the water area below the river mouth, which reduces the tsunami run-up intensity. The most efficient solution for bridges across narrow rivers is a single-span structure without an intermediate support. Thus, tsunami bridge protection is ensured by the choice of the bridge location and its constructive design and, if necessary, by engineering structures that reduce the calculated tsunami intensity. As for bridges and, in general, transport routes located along tsunami-prone coasts, they are usually designed on a high bench, well protected by bank protection structures. An example of such a highway is the Lisbon-Cabo da Roca highway. If possible, such highways are separated from the coastline by a “soft” buffer (forest plantations), which, in the conditions of the Russian Far East, protects railways from an unacceptable snowdrift. In practice, on the THA, sections of the coastal railway are so narrow (pressed against steep mountainous terrain) that it is impossible to ensure tsunami safety on them. Therefore, in accordance with the norms [49], on both sides of such sections, it is recommended to provide dead-end railway branches leading to the safe zone, where the train has time to move after receiving an alarm notification from the TSC. As for the railway track, its destruction is considered acceptable and requires urgent repair. Corresponding recommendations were issued to the management of Russian Railways for implementation on the railway operated on the Okhotsk Sea Coast of Sakhalin Island where such sections are found.

Urban planning aspects of tsunami safety management are highlighted in Set of Rules 292 in a special, important section, the development of which takes into account the domestic experience of transferring the village of Ust-Kamchatsk, located on the eastern coast of the Kamchatka Peninsula and affected by the 1923

and 1952 tsunamis, to a high inaccessible to the calculated tsunami place – the village of Krutoberegovo, as well as urban planning measures taken on the islands of the Kodiak archipelago for tsunami protection in the 1960s after the 1946 and 1964 tsunamis. In addition, planning errors that adversely affected the disaster magnitude from the 2004 Indian Ocean tsunami were taken into account [6, 7, 12, 58].

The key object of standardization is the SESURB, the main part of which is the THA, which requires regulatory regulation of at least two standardization aspects: a parameter that characterizes and ensures the preservation of human life and health and a parameter that characterizes and ensures that an acceptable level of material and environmental damage is not exceeded in the event of the estimated tsunami impact.

The basis for developing a tsunami safety strategy for a particular THA is a reasonable ranking of the tsunami safety regulation zone into subzones of various tsunami exposure degrees. To do this, it is recommended to assign the THA subzones, differentiating them by the maximum height of the expected tsunami flow once every 500 years, according to the DEM results and the flow velocity in each subzone. As a result, using the tsunami intensity scale (Table 1), the flood zone is divided from top to bottom into subzones with different  $I_{ts} = 0, I, II, III \dots, \max I_{ts}$ , which is used in the SESURB seaside planning and development project to provide coastal community resilience. The SESURB regulation outside the flood zone is generally mandatory for the hard-to-evacuate THAs including those with nearby tsunamis. All buildings located within the flood zone must be inventoried and certified with the description of their design scheme and the indication of the responsibility degree, the category of constructive vulnerability [37, 47], and the level of functional vulnerability for key facilities under the tsunami influence, as well as the indication of the allowable material damage to the building, set by the owner. In the process of certification, it is necessary to single out the most well-studied, calculated in detail (taking into account the interaction in the “structure–soil” system) and located on the coast under the instrumental control of the building-BAOBAB. At the same time, the BAOBAB-like SIB buildings are described on similar seacoasts around the world, the reaction of which to the tsunami impact is well-studied. All BAOBABs and SIBs will be considered together in the subsequent tsunami risk analysis. On seacoasts with predicted local tsunamis, the designated BAOBABs and selected SIBs should be additionally certified for all SESURBs in terms of their seismic resistance [47]. For each subzone in Set of Rules 292, the recommendations are given on the restrictions on the use of this subzone, the need to arrange a soft “buffer (forest plantations, park areas) or a ‘hard’” protective buffer (wave protective bank protection structures), transferring some part of buildings of a certain purpose and responsibility to a less dangerous zone, specific requirements and recommendations to improve the resistance of buildings to the tsunami effects, advice on land use, evacuation of valuables, advice to owners on property insurance, etc. Particular attention is paid to measures to prevent the appearance and entry of debris into tsunami waves, which significantly increase their destructive ability. These measures include moving surface car parks above the flood line, increasing the underground garage construction, minimizing the amount

of potential debris in the flood zone, regulating the shape, roughness, and wear resistance of the road surface descending to the sea, and gaps in frontal coastal development to counteract the ingress of this debris and debris into the second and third waves during the tsunami outflow, as well as the ingress of ice fragments during the run-up into the urbanized area. Flood-affected areas are not recommended for newly developed areas or residential buildings. In areas prone to flooding, safety should be ensured by the lattice platform construction with supporting parts in the form of spatial trusses for vertical evacuation. Particular attention should be paid to the protection of water supply and sewerage in urban areas and the prevention of environmental damage, since, for example, wastewater treatment plants are always located close to sea level. Transportation systems must be capable of rapid mass evacuation from flooded areas. These issues are discussed, for example, in [1, 8].

Thus, the urban planning strategy for tsunami safety includes not only planning activities, but also targeted design solutions, as well as measures for engineering territory protection. The effectiveness of a wide range of these activities is assessed by using mathematical modeling of Disaster Scenario for CONTROL (DISCONT) when Disaster Scenario (DISC) includes certain suggested activities [29].

### ***3.5 Scenario Approach to Disaster Analysis, Management, and Monitoring***

The use of the scenario approach for the tsunami risk, i.e., a probable disaster analysis (the PRANA subprogram) and management (the PRIMA subprogram), is the clearest, most convenient and effective mechanism to ensure sustainable security ultimately, including coastal community resilience. The development of disaster scenarios begins with the compilation of the initial and updated AMFORA database and the probable scenario set of the complex hazard scenario of the expected tsunami, mandatory for each tsunami hazardous area, taking into account parallel and secondary hazards. In this case, the night and transport scenarios are usually selected, which are usually the worst. Then, within this area, the interaction of offshore hydraulic structures and coastal buildings with a package of three individual tsunami waves is modeled, and the loads and impacts on the objects under consideration at the tsunami hazardous area, including existing and planned engineering protection structures, are specified. In the process of this work, the risk subject vulnerability (the population, the structural and functional vulnerability of buildings, and structures for various purposes and constructive types) located within the social–economic system of urbanization (SESURB) to the probable hazards accompanying the tsunami is analyzed. The corresponding GIS for Vulnerability City Analysis (“VULCAN”) is formed [47, 48]. Simultaneously, on the considered THA and SESURB, identical BAOBABs erected on sites with different soil conditions are identified as the development representatives, and then, as a result of a special search, objects that are similar building analogs are



added to these BAOBABs. Basic and analog objects are included in BANKNOTES (BANK of KNOWledge, Testing and Experience in the Safety). Processing of the dependence “tsunami intensity - vulnerability - damage to buildings” is carried out by using the well-proven mathematical method MELESA (Method of Expert-Logical Estimations and System Analysis). The DAMESTEC (DAMAGE ESTimation TECHnique) method is used to assess damage and loss of life, including the Loss ESTimation Technique (LEST) in the second stage. This highlights buildings that can kill many people, due to progressive collapse (PROCOL) as a result of the initial local damage from a low-level load. The results of human losses and material damage analysis are used to assess the disaster parameters according to the Disaster Magnitude Scale (DIMAK) described in paragraph 4. These results, together with other standard parameters and features, are entered into the GIS “DISC.” DISCONT is used to test the effectiveness of alternative protective measures and select the best design solution. At the same time, the risk indicators, obtained in the DISCONT, are compared with the individual, collective, and economic PERmissible Risk Level (PERIL), which are established by standard [15] or by the building owner. The economic risk takes into account direct, secondary, and indirect material damages separately, including compensation costs for the environmental damage restoration. The complex risk assessment is done based on the probabilistic analysis of secondary and/or parallel hazardous natural and anthropogenic impacts associated with the tsunami. With the help of the DISCONT, constant monitoring of the seaside/coastal SESURB safety is carried out, as well as the site selection for the placement of potentially dangerous objects designed on the seacoasts. After each working DISC, the probable disaster parameters are estimated according to the DIMAK scale, and/or AGgregate Risk Analysis (AGRA) is performed, the results of which can be presented both in a numerical and in a graphical representation. As an example, [45] presents the total disaster risk map of the Krasnodar Territory, Russia (Fig. 4).

The procedure for performing AGRA (AGgregate Risk Analysis) is based on papers [29, 33, 38, 39]; the schematic diagram of the security control analysis of urban areas subject to uncontrolled natural impacts is shown in Fig. 5.

As part of the initial disaster mitigation block (MIT block), based on the worst DISC for each SESURB, preparedness and the READiness SCenarios (READISC) are developed, including the forces and means necessary to eliminate the emergency, places, ways, and procedures for evacuating the population and the corresponding plans for probable emergency rescue operations, as well as emergency life support plans for the population (Disaster & Emergency medicine, energy, heat and water supply, shelter, and food provision). The READiness SCenarios (READISC) is being developed as a continuation of the DISC on the same geo-information platform.

In addition, it is necessary to develop alternative rehabilitation and recovery scenarios for the victim SESURB. The REcovery SCenario (RECS) includes the rehabilitation scenario (REHABS) and the reconstruction scenario (RECONS). The development of preliminary scenarios and relevant methodological/recommendatory documents for the affected coastal community rehabilitation





Fig. 4 Aggregate disaster risk map. (Krasnodar Krai, Russia 2005)

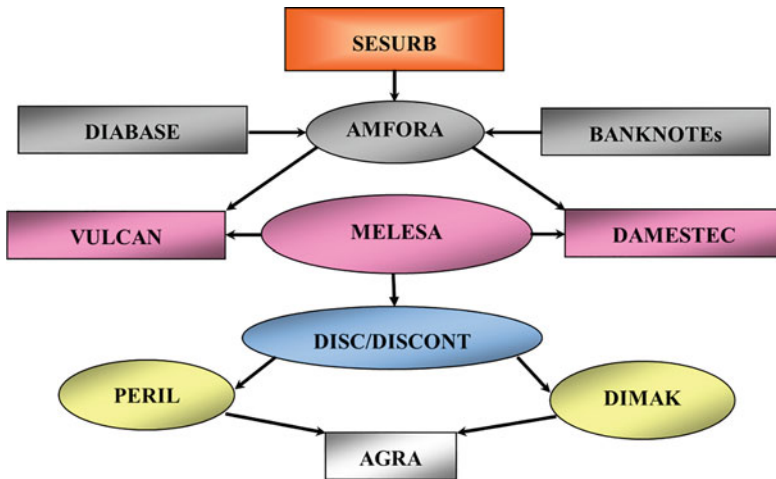


Fig. 5 Disaster risk analysis and control scheme for hazardous natural impacts

(full and long-term life support for the population, correct homeless resettlement, the banking system and business restoration, etc.), as well as for the reconstruction of damaged buildings and structures, including renovation and construction of new buildings are being discussed nowadays. An example is the planning and assistance in the implementation of such work after the devastating earthquake and the 2011 Tohoku tsunami [20]. During the same period (if justified), the special structure creation for engineering protection against tsunamis (“soft” and “hard” buffer) is carried out, and urban planning is improved for safety purposes. The effectiveness of each virtual protective/rehabilitative/restorative action is evaluated by using the disaster scenario for control (DISCONT) that is followed by the cost–benefit analysis.

### **3.6 Special Policy on THA**

In addition to the engineering and planning measures described above, in the disaster reduction strategy for the seacoasts affected by the tsunami, an important place is occupied by the following:

- The land use regulation in the tsunami hazardous area and often in social–economic system of urbanization (SESURB), compiling a special cadaster, dangerous for the coastal land infrastructure development, restricting construction land development, prohibiting and/or restricting new development of dangerous coastal areas, stimulating and compensating the demolition, and relocation of existing residential and civil buildings to higher, safer places.
- Special differentiated taxation on property in the tsunami hazardous area.
- A legislative order to the owners of coastal enterprises, the transfer of which from the tsunami hazardous area is impossible (fish-receiving industries, ship repair enterprises, etc.), to take guaranteed measures to prevent dangerous secondary industrial tsunami consequences (replace ammonia in freezers with freon, additionally protect pipelines with hazardous reagents, improve the emergency warning system and technical supervision), and increasing their responsibility in case of violation.
- Insurance/reinsurance development for probable loss of people’s life and health, reduction in the breadwinner’s ability to work, damage to housing and property, damage to career growth, business activity and business, and environmental damage due to the disaster tsunami and related parallel and secondary impacts.

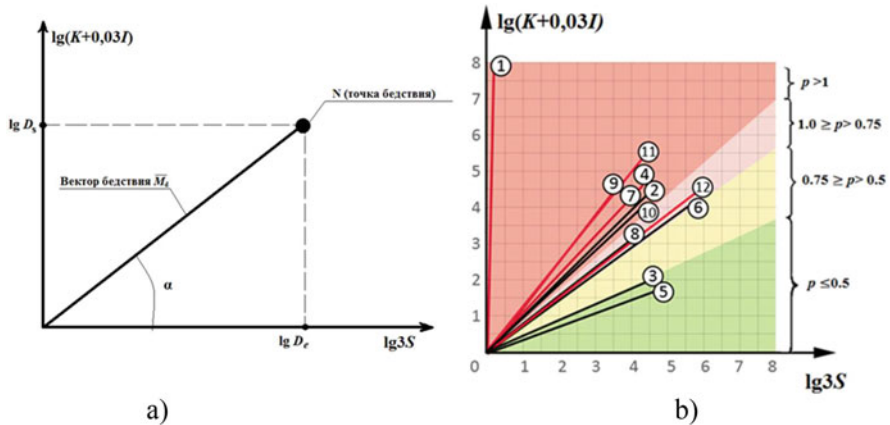
The developed code of rules for the structure design in the tsunami hazardous zone is used in specific engineering projects carried out in Russia.

## 4 The Disaster Magnitude Scale “DIMAK”

Tsunamis are one of the causes of natural disasters. It is impossible to assess the severity of any disasters, to manage disasters by reducing them, to realize their social and economic impact on the population and territories of various countries, and to understand what disasters are permissible, acceptable, and can be eliminated by the own forces and means of the affected territory (without outside help), it is impossible to talk about disasters at all and, moreover, to establish state norms for the maximum permissible disaster parameters for countries with different economic potential without unified and regulated quantitative disaster parameters, that is, without the ability to measure these disasters clearly and unambiguously. After the 1988 Tokyo Declaration, the understanding of the need for a disaster scale increased significantly, the first proposal in the world was Prof. A.Z. Keller’s proposal from the University of Bradford (U.K.), who proposed a six-level scale that depends on one disaster parameter – the number of people killed. The Bradford Disaster Scale (BDS) is based on the logarithm of the number of fatalities involved in the disaster occurrence [25]. Thus, with the help of the BDS, six disaster levels (from 1 to 6) can be represented, the consequences of which are the death of 10,  $10^2$ ,  $10^3$ ,  $10^4$ ,  $10^5$ , and  $10^6$  people, respectively. The BDS has been used to quantify and qualify chemical disasters. Later, the BDS was used in the same way as the model to assess disasters in terms of total economic losses. It was clear that such a model could not simultaneously take into account the death and injury of people, their suffering, economic loss, and environmental damage, that is, to measure the disaster as a whole. That is why a two-dimensional vector model is used in the scale of disaster magnitude that has been developed by Klyachko (see, e.g., [30, 32, 40]). The DIMAK disaster scale was developed and tested on the consequences of the 1988 Spitak earthquake (Armenia) and the 1990 Manzil earthquake (Iran). The DIMAK scale makes it possible to evaluate the parameters of any natural or manmade disaster, to control in the monitoring mode the size of disaster consequences predicted by using disaster scenario, and to manage disaster risk by evaluating the effectiveness of certain measures for sustainable safety provisions [33].

The initial indicators in the DIMAK disaster scale are i) the number of dead (irretrievable losses)  $K$ , ii) the number of injured (sanitary losses)  $I$ , and iii) the amount of financial losses  $S$ , million US dollars. The main parameters of the DIMAK distress scale are as follows:

- The distress magnitude  $M_d$  is measured by the length of the beam (vector)  $ON$ , where  $O$  is the zero point (the origin of orthogonal coordinates) and  $N$  is the distress point (Fig. 6). Depending on the magnitude, disasters are subdivided into inconspicuous ( $<1.0$ ), insignificant (1.0–2.5), significant (2.5–4.5), large (4.5–6.0), severe (6.0–7.0), and catastrophe ( $\geq 7$ ).
- The relative social vulnerability index  $p = \tan \alpha$ , where  $\alpha$  is the angle between the  $ON$  ray and the abscissa axis. If  $p = \infty$ , the disaster is said to be “entirely social,” and if  $p = 0$ , the disaster is said to be “purely economic.” Depending on the value of  $p$ , disasters are categorized according to the acceptability degree:



- 1 - Plague, Europe, 1337-1352,  $M_d = 7.8$ ;  $p = \max$  (pure social disaster)
- 2 - Spitak earthquake, Armenia, USSR, 07.12.88,  $M_d = 6.45$ ;  $p = 0.94$
- 3 - Loma Prieta earthquake, California, USA, 17.01.89,  $M_d = 4.80$ ,  $p = 0.42$
- 4 - Manjil earthquake, Iran, 21.06.90,  $M_d = 6.3$ ;  $p = 1.06$
- 5 - Northridge earthquake, California, USA, 17.01.94,  $M_d = 4.93$ ;  $p = 0.38$
- 6 - Big Khanshin earthquake, Kobe, Japan, 17.01.95,  $M_d = 6.67$ ;  $p = 0.68$
- 7 - Izmit Earthquake, Turkey, 17.08.99,  $M_d = 5.75$ ;  $p = 1.06$
- 8 - Chi-Chi Earthquake, Taiwan, 21.10.99, 04.10.94,  $M_d = 5.15$ ;  $p = 0.83$
- 9 - Bhuj Earthquake, Gujarat, India, 27.01.01,  $M_d = 5.64$ ;  $p = 1.17$
- 10 - Terrorist attack, New York, USA 11.09.01,  $M_d = 5.52$ ;  $p = 0.9$
- 11 - Port-au-Prince Earthquake, Haiti, 12.01.10,  $M_d = 6.88$ ;  $p = 1.24$
- 12 - Tohoku Earthquake and tsunami, Japan, 11.03.11,  $M_d = 7.06$ ;  $p = 0.68$

**Fig. 6** Graphic representation of a single disaster  $N$  (a) and “the disaster field” of 12 disaster events (b)

with  $p < 0.25$  – absolutely acceptable for all countries; at  $p < 0.5$  – acceptable for developed countries; at  $p < 0.75$  – acceptable for developing countries; at  $p < 1$  – inadmissible; and for  $p > 1$ , they are absolutely inadmissible.

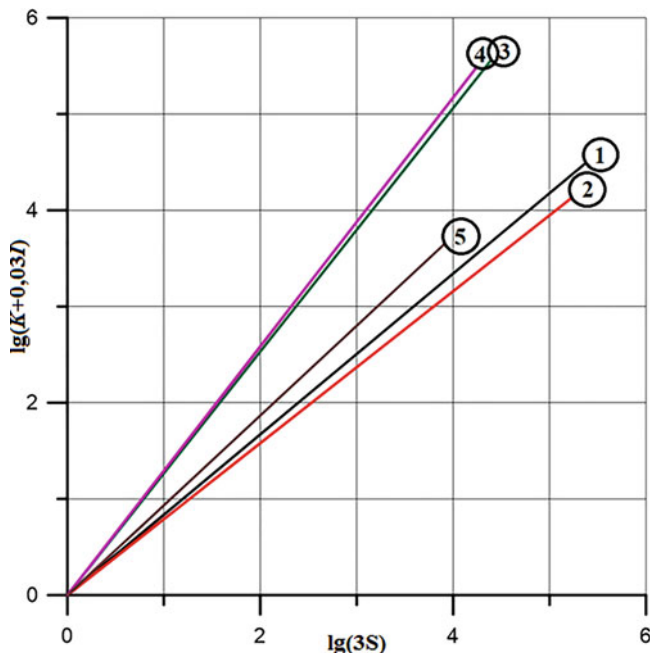
To assess the economic possibility of the affected territory to eliminate the emergency situation on its own and recover from the disaster, an additional index of economic stability  $d_m$  is used.

$$d_m = \frac{D_s + D_e}{G}, \tag{7}$$

where  $D_s$  and  $D_e$  are, respectively, the size of social losses and economic damages in monetary terms.

$G$  – GDP of the affected administrative entity (local, country, federal) for the year preceding the disaster.

The  $d_m$  indicator characterizes the ability of the affected area for rehabilitation and recovery, which emphasizes the fact that resilience, or sustainable safety, must



1. Tsunami 27.12.2004 (except Indonesia): 228000 fatalities, 10000 million USD loss;  $M_d = 6.98$ ;  $p = 0.7$
2. Tsunami 27.12.2004 (Indonesia): 167540 fatalities, 4 450 million USD loss;  $M_d = 6.66$ ;  $p = 0.67$
3. Tohoku Tsunami 11.03.2011 (tsunami and earthquake): 23000 fatalities, 6245 injured, 122000 million USD loss;  $M_d = 7.09$ ;  $p = 0.90$
4. Tohoku Tsunami 11.03.2011 (only tsunami): 16000 fatalities, 4000 injured, 100000 million USD loss;  $M_d = 6.92$ ;  $p = 0.91$
5. Tsunami 28.09.2018: 4340+667 fatalities, 10679 injured, 1500 million USD loss;  $M_d = 5.35$ ;  $p = 0.75$

**Fig. 7** Parameters of tsunami disasters of 2004, 2011, and 2018 in different countries

be constantly maintained, which is provided by money capacity and insurance. The relative level of the territory economic potential in terms of its ability to recover is described in terms of the relative scale of the disaster that occurred, namely facility, municipal/city, territorial, national, regional, and global scale.

It is convenient to use the graphical interpretation to illustrate the main distress parameters. Figure 6a shows point *N*, called “the disaster point” with the corresponding parameters, while Fig. 6b shows a collection of different disasters, called the “disaster field,” accompanied by the values of their main parameters.

Figure 7 shows that the 2004 and 2011 tsunamis caused disasters of the “catastrophic” ( $M_d \geq 7$ ) category according to the DIMAK scale. At the same time, the index of social vulnerability of the tsunami disaster of 2011 is so large that this calamity belongs to the category of “unacceptable.” In the case of the Tohoku Tsunami, as the index of economic stability  $d_m$  (formula 7) shows, recovery after such calamity could be quite a feasible task even at the local level, and the participation of national economic capacity has accelerated the recovery process. As for the 2004 and 2018 tsunamis in Indonesia, the happened disasters are classified as the “severe,” but as “acceptable for developing countries” ones. However, to recover

from these disasters, the local economic capacity is not enough national assistance is needed, because otherwise the complete recovery of the affected area will take an unacceptably long time.

In the next section, we will give the disaster magnitude estimates for one area in Russia where the predicted earthquake was controlled.

## 5 Case Study

As an application of the technology described above, we present here the hazard forecast, analysis, and forecast disaster management in Kamchatka (Russia), carried out in 1986–2002. In 1985, a group of seismologists from the Institute of Volcanology made a medium-term forecast of a devastating earthquake with an epicenter in Avacha Bay of the Pacific Ocean, 70 km from Avacha Bay, on the coast of which the capital of the Kamchatka Region, Petropavlovsk–Kamchatskiy, the cities of Yelizovo and Vilyuchinsk are located (Fig. 8).

This forecast was taken very seriously at the government level, and the Decree of the Russian Government No. 2359-R “On Ensuring the Seismic Resistance of the National Economy Objects of the Kamchatka Region” (dated 21.11.1986) appeared, later supported by other, additional government decrees indicated earlier. The Institute of Physics of the Earth (Moscow) has developed the six probable earthquake scenarios foreseeing the possibility of a seismogenic tsunami. Scientific and design work was entrusted to the Institute CENDR. To implement

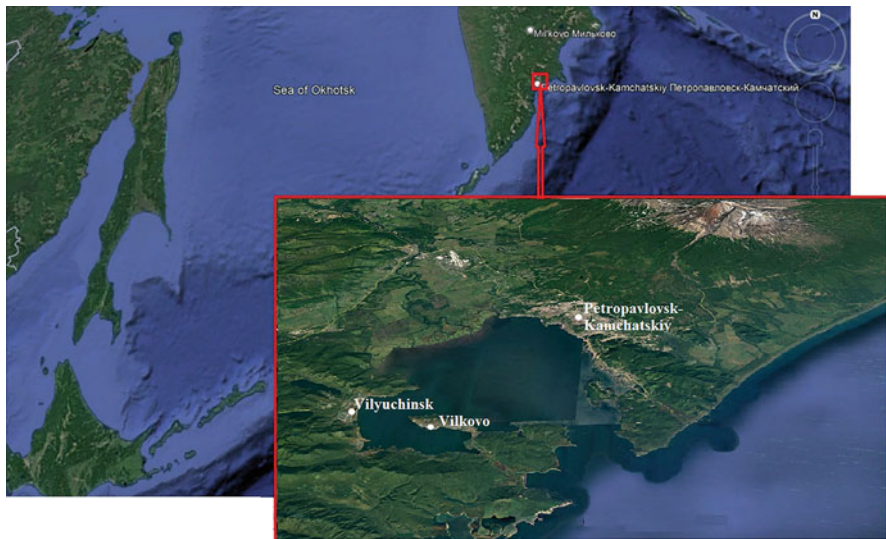


Fig. 8 Map of study area



the government decisions, CENDR developed and consistently implemented the subprogram of risk analysis (PRAHA) and, then, through the joint Russian–Yugoslavia enterprise JV “Adriakampacifik,” the subprogram of risk management (PRIMA) [34], having formed by 1995, the Federal Center for Public Utilities Seismic Protection “Seismoprotection.”

In relation to the tsunami presuming the interest to us, two worst seismogenic events were considered – the epicenter of the earthquake  $M = 7.8$  in Avacha Bay (working hazard scenario) and the epicenter  $M = 7.8$  in Avacha Bay (rejected due to the incredible destructive ability and the frequency of once in 20,000 years). The working hazard scenario is represented by the tsunami with a run-up height of 15 m, threatening Petropavlovsk–Kamchatsky from Khalaktyrsky Beach, and the entire urbanized area around Avacha Bay from the entrance side to this bay. Based on the hazard scenario results and the corresponding disaster scenarios, the tsunami run-up probabilistic model from the Khalaktyrsky Beachside was constructed [22]. As for the urbanized area around Avacha Bay, and first of all, Petropavlovsk–Kamchatsky, in the corresponding hazardous scenario, the bays of Babia, Rakovaya (heights 5–6 m), the seaport territory, the station, and the refrigerator were noted as the most dangerous ones, and also as less dangerous, exploited coasts of Seroglazka village and the Avachinsky fish processing plant. The flooding scenario of the Petropavlovsk–Kamchatsky urban area was adopted similarly to the consequences of the catastrophic 1952 tsunami. The order was issued to improve the seismic and tsunami safety of the maritime station building and to replace immediately ammonia with freon in a multi-stored refrigerator in order to reduce the risk of poisoning the population. Based on disaster scenario, the Far Eastern Association “Reliability and Security,” together with the “Center for Research in Extreme Situations,” developed the GIS “Extremum,” containing response scenarios and performed calculations of the forces and means necessary to eliminate emergencies [44]. This study was awarded the first prize of the Russian Emergency Situations Ministry. At the same time, improved and locally oriented reminders for the population on preparing for a possible natural disaster were developed; moreover, a weekly hour-long TV training program “Seismic Alarm Clock” was organized with answers to questions from the population, as well as a practically very useful Association “Let’s save ourselves with our own hands” was organized. By using the DIMAK distress scale, the subprogram of risk management (PRIMA) implementation was monitored, some intermediate results of which are shown in Table 2.

Thus, a comprehensive disaster risk analysis and management program was successfully implemented in the practical safety of Petropavlovsk–Kamchatsky, which got ready for the predicted earthquake and became a donor in the RADIUS project announced by UNESCO for the period from 1994 to 1999 to diagnose and prepare the world’s cities for an earthquake. Unfortunately, far from the entire part of the PRESS program related to tsunami protection was carried out in Petropavlovsk–Kamchatsky and Vilyuchinsk, it happened mainly due to the lack of modern computer technologies for mathematical modeling, as well as due to insufficient awareness of the need to timely and continuously increase tsunami safety of the urbanized seacoasts. Intermediate disaster management results predicted in

**Table 2** EQ disaster assessment

Period	EQ consequences						DIMAK Scale scores		
	Killed	Injured	Homeless	Total losses (\$, mln)	$M_d$	Terms for disaster description	Score of disaster permissibility		
Before PRESS, 1990	3000	14,000	100,000	8000	5.63	Major disaster of national scale	Unacceptable		
During PRESS, 1st stage, 1995	2000	6000	65,000	4200	5.29	Major disaster of national scale	Unacceptable		
During PRESS, 2nd stage, 1999	200	1500	9000	1200	4.29	Disaster of territorial scale	Semi-acceptable		
During PRESS, 3rd stage, 2002	50	200	5000	1000	3.95	Disaster of local scale	Permissible		



Kamchatka were demonstrated at conferences on earthquake engineering (1994, Vienna, Austria; 1998, Paris, France; 2000, Auckland, New Zealand).

The strong Kronotsky earthquake of December 5, 1997,  $M = 7.7$ , was the best natural test that proved the high efficiency of the Preventive Seismic Safety (PRESS) Program implemented in Kamchatka: The category of structural vulnerability of reinforced buildings became 1–2 steps lower than the vulnerability values of these buildings before their reinforcement.

## 6 Conclusion

The basis of disaster risk management to ensure coastal community resilience is the decision of the 1988 Tokyo Declaration, the world experience in disaster mitigation during the International Decade of Natural Disaster Reduction (IDNDR), as well as the recommendations of the world conferences on disaster reduction in Yokohama (1994), Kobe (2005), and, finally, Sendai (2015).

Tsunami risk awareness, understanding, and management are becoming an important and urgent task, not only in terms of preventing human casualties but also in terms of minimizing material and environmental damage. That is why the improvement and implementation of the tsunami safety concept provides us with a step-by-step, consistent path for sustainable coastal community development.

The way to manage a tsunami disaster is to reduce the structural and functional vulnerability of building structures, as well as the planning vulnerability of coastal urban areas. Considering the fact that tsunamis are rare and impossible to control, the most important task is to survey the tsunami disaster consequences with a significant increase in the number of professional hydraulic engineers, geotechnical engineers, and civil engineers. Based on the practical results of the engineering survey and the lessons learned, it is necessary to improve building codes for tsunami protection of urbanized seacoasts and train practical design engineers. At the same time, a special task is to assign the basic objects for tsunami safety analysis at each tsunami hazardous area and select the analog objects necessary to increase the decision reliability made when developing probable disaster scenarios.

The consequences of a local seismogenic tsunami with ice inclusion should be recognized as the most destructive disaster, which in areas with a cold climate should be taken as the maximum impact, firstly, at objects of increased responsibility. Since debris in a tsunami flow significantly and in a wide range affects the tsunami destructive ability, the best strategic goal is to prevent completely any debris from entering the tsunami flow. An exception to this rule is to prevent ice, the appearance of which in a tsunami flow in regions with a cold climate is very difficult. The issue of protecting bridges from the ice tsunami impact is resolved in the developed Russian Set of Rules 292. As for the prevention of huge economic and environmental losses similar to the consequences of the 1923 and 1952 Kamchatka tsunamis, the problem of tsunami safety is obviously solved based on a cost–benefit

analysis in a different range: from complete or partial refusal to develop a tsunami-prone coast to the construction of engineering protection structures of various levels.

It should be noted that, despite the world's best tsunami warning system in Japan, and, as it seems, historically high people's preparedness for the tsunami, including their correct reaction knowledge, the Tohoku tsunami drowned more than 14,000 people; that is, the world system tsunami warnings, in general, requires significant improvement.

Because tsunamis are a very rare natural event, experience gained directly from the results of engineering surveys of tsunami disasters is slowly accumulating. That is why the results of natural and laboratory physical modeling of the tsunami interaction with various structures are becoming more and more important and fruitful. Therefore, this scientific and experimental direction should be developed everywhere and as a priority.

The most tsunami-vulnerable structures are aseismic developments, which are only susceptible to distant tsunamis. The use of high coastal buildings for vertical evacuation is allowed only in the case of the seismic isolation of these buildings, since otherwise the requirements for the people's evacuation during the earthquake and the tsunami will be contradictory.

In our opinion, it is necessary to create the vulnerability and damageability catalog of analog objects of the housing stock affected by the tsunami based on the engineering survey results of the consequences of damaging and destructive tsunamis that occurred in the world. It should be done to complete the database necessary for developing disaster scenarios on seacoasts that do not have their own tsunami experience. It is necessary to develop the Eurocode "Design of structures for tsunami resistance" under the auspices of the European Association for Earthquake Engineering (EAEE).

The preventive sustained safety program (PRESS) developed by CENDR, contained special tools to analyze and reduce disasters caused by earthquakes and tsunamis, was successfully implemented in the form of a consistent roadmap for the urbanized area around Avacha Bay (Kamchatka, Russia). It made the PRESS program a reference in the UNESCO project "RADIUS" and in the joint project "U.S. West Coast - Russian Far East: STOP Disaster" (1994–2001). These approaches and tools have been successfully applied to analyze probable disasters in many other territories of the constituent entities of the Russian Federation (Federal Program "SeismoSafety") and in the Commonwealth of Independent States (CIS) countries (Program "Seismopolis").

## 7 Nomenclature

A significant number of abbreviations are used in the present paper; for ease of perception and reading, they are presented in Table 3. Abbreviations accompanied by a detailed concept in the text are not included in the table given below.

**Table 3** Computer Associative Logical Abbreviations for Mitigation of Calamities (CALAMIC)

Abbreviation	Concept
AMFORA	Applicate Material for FORMula of Risk Analysis (FORA)
BANKNOTES	BANK of KNOWledge, Testing and Experience in the Safety
BAOBAB	BAasic OBjects for Analysis of Buildings
CENDR	FSUE “R&D Centre on Earthquake Engineering and Natural Disaster Reduction”
DIABASE	Informatics – Analytics DataBASE
DIMAK	DISaster MAGnitude of Klyachko
DISC	DISaster Scenario
DISCONT	DISaster SCenario for CONTrol
PRANA	Program of Risk ANALysis
PRESS	PREventive Seismic Safety
PRIMA	Program of RISK Management
SESURB	Social–Economic System of URBanization
SIB	Similar Buildings

**Acknowledgments** AZ had a support from the State Task of Special Research Bureau for Automation of Marine Researches ‘Coastal risks related to natural disasters taking into account engineering and social-economics applications’, EP and TT - the support from the Laboratory of Nonlinear Hydrophysics and Natural Hazards, V.I. Il’ichev Pacific Oceanology Institute, grant of the Ministry of Science and Higher Education of the RF, ag. No. 075-15-2022-1127.

## References

1. Asgarizadeh, Z., Gifford, R.: Community and psychological barriers to tsunami preparation. *Nat. Hazards*. (2022). <https://doi.org/10.1007/s11069-022-05228-8>
2. Aytore, B., Yalciner, A.C., Zaytsev, A., Cankaya, Z.C., Suzen, M.L.: Assessment of tsunami resilience of Haydarpaşa Port in the Sea of Marmara by high-resolution numerical modeling. *Earth Planets Space*. **68**, 1–12 (2016)
3. Basili, R., Brizuela, B., Herrero, A., Iqbal, S., Lorito, S., Maesano, F.E., Murphy, S., Perfetti, P., Romano, F., Scala, A., Selva, J., Taroni, M., Thio, H.K., Tiberti, M.M., Tonini, R., Volpe, M., Glimsdal, S., Harbitz, C.B., Løvholt, F., Baptista, M.A., Carrilho, F., Matias, L.M., Omira, R., Babeyko, A., Hoechner, A., Gurbuz, M., Pekcan, O., Yalçiner, A., Canals, M., Lastras, G., Agalos, A., Papadopoulos, G., Triantafyllou, I., Benchekroun, S., Agrebi Jaouadi, K., Ben Abdallah, S., Bouallegue, A., Hamdi, H., Oueslati, F., Amato, A., Armigliato, A., Behrens, J., Davies, G., Di Bucci, D., Dolce, M., Geist, E., Gonzalez Vida, J.M., González, M., Macías Sánchez, J., Meletti, C., Ozer Sozdinler, C., Pagani, M., Parsons, T., Polet, J., Power, W., Sørensen, M.B., Zaytsev, A.: The making of the NEAM Tsunami Hazard Model 2018 (NEAMTHM18). *Front. Earth Sci.* **8**, 591549 (2021)
4. Behrens, J., Løvholt, F., Jalayer, F., Lorito, S., Salgado-Gálvez, M.A., Sørensen, M., Abadie, S., Aguirre-Ayerbe, I., Aniel-Quiroga, I., Babeyko, A., Baiguera, M., Basili, R., Belliazzi, S., Grezio, A., Johnson, K., Murphy, S., Paris, R., Rafliana, I., De Risi, R., Rossetto, T., Selva, J., Taroni, M., Del Zoppo, M., Armigliato, A., Bures, V., Cech, P., Cecioni, C., Christodoulides, P., Davies, G., Dias, F., Bayraktar, H.B., González, M., Gritsevich, M., Guillas, S., Harbitz, C.B., Kanoglu, U., Macías, J., Papadopoulos, G.A., Polet, J., Romano, F., Geist, E.L., Parsons,

- T.: Probabilistic analysis of tsunami hazards. *Nat. Hazards*. **37**, 277–314 (2016)
5. Belyaev, N., Lebedev, V., Nudner, I., Semenov, K., Schemelinin, D.: Method for calculating extreme loads on a floating object from the direct impact of tsunami waves based on experimental studies. *Hydraul. Eng. Construct.* **3**, 46–50 (2022). <https://doi.org/10.34831/EP.2022.31.74.007>. (in Russian)
  6. Castro, S., Poulos, A., Herrera, J., Llera, J.: Modeling the impact of earthquake-induced debris on tsunami evacuation times of coastal cities. *Earthquake Spectra*. **35**, 137–158 (2019). <https://doi.org/10.1193/101917EQS218M>
  7. Chang, S., Adams, B., Alder, J., Berke, P., Chuenpagdee, R., Ghosh, S., Wabnitz, C.: Coastal ecosystems and tsunami protection after the December 2004 Indian Ocean tsunami. *Earthquake Spectra*. **22**, 863–887 (2006). <https://doi.org/10.1193/1.2201971>
  8. Chen, C., Mostafizi, A., Wang, H., Cox, D., Cramer, L.: Evacuation behaviors in tsunami drills. *Nat. Hazards*. (2022). <https://doi.org/10.1007/s11069-022-05208-y>
  9. Chock, G., Carden, L., Robertson, I., Olsen, M., Yu, G.: Tohoku tsunami-induced building failure analysis with implications for U.S. tsunami and seismic design codes. *Earthquake Spectra*. **29**, 99–126 (2013). <https://doi.org/10.1193/1.4000113>
  10. Didenkulova, I.I., Pelinovsky, E.N.: Phenomena similar to tsunami in Russian internal basins. *Russ. J. Earth Sci.* **8**, ES6002 (2006)
  11. Dogan, G., Yalciner, A., Yuksel, Y., Ulutaş, E., Polat, O., Güler, I., Şahin, C., Tarih, A., Kanoğlu, U.: The 30 October 2020 Aegean Sea tsunami: post-event field survey along Turkish coast. *Pure Appl. Geophys.* **178**, 785–812 (2021). <https://doi.org/10.1007/s00024-021-02693-3>
  12. Edwards, C.: Thailand lifelines after the December 2004 great Sumatra earthquake and Indian Ocean tsunami. *Earthquake Spectra*. **22**, 641–659 (2006). <https://doi.org/10.1193/1.2204931>
  13. Gibbons, S.J., Lorito, S., Macias, J., Løvholt, F., Selva, J., Volpe, M., Sánchez-Linares, C., Babeyko, A., Brizuela, B., Cirella, A., Castro, M.J., de la Asunción, M., Lanucara, P., Glimsdal, S., Lorenzino, M.C., Nazaria, M., Pizzimenti, L., Romano, F., Scala, A., Tonini, R., Manuel González Vida, J., Vöge, M.: Probabilistic tsunami hazard analysis: High performance computing for massive scale inundation simulations. *Front. Earth Sci.* **8**, 591549 (2020)
  14. Gonzalez, F.I., Geist, E.L., Jaffe, B., Kanoglu, U., Mofjeld, H., Synolakis, C.E., Titov, V.V., Arcas, D., Bellomo, D., Carlton, D., Horning, T., Johnson, J., Newman, J., Parsons, T., Peters, R., Peterson, C., Priest, G., Venturato, A., Weber, J., Wong, F., Yalciner, A.: Probabilistic tsunami hazard assessment at Seaside, Oregon, for near- and far-field seismic sources. *J. Geophys. Res.* **114**, C11023 (2009)
  15. GOST R 55059-2012 (Russian national standard). Safety in emergencies. Emergency risk management. Terms and definitions
  16. GOST 27751-2014. (Russian national standard) Reliability for constructions and foundations. General principles
  17. Gusiakov, V.K., Kikhtenko, V., Chubarov, L.B., Shokin, Y.: Regional tsunami hazard maps for the Far East coast of Russian Federation built in the framework of the PTHA methodology. *Comput. Technol.* **24**, 55–72 (2019)
  18. Ishihara, K.: *Soil Behavior in Earthquake Geotechnics* Oxford Engineering Science Series, p. 385. Clarendon Press (1996)
  19. Ivashenko, A.I., Gusyakov, V.K., Dzhumgaliev, A., Yeh, H., Zhukov, L.D., Zolotukhin, N.D., Kaistrenko, V.M., Kato, L.N., Klochkov, A.A., Korolev, Y.P., Kruglyakov, A.A., Kulikov, E.A., Kurakin, V.M., Levin, B.V., Pelinovskii, E.N., Poplavskii, A.A., Titov, V.V., Kharlamov, A.A., Khrumushin, V.M., Shelting, E.V.: The Shikotan tsunami of October 5, 1994. *Transactions (Doklady of the Russian Academy of Sciences). Earth Sci. Sect.* **348**, 693–699 (1996)
  20. Iuchi, K., Johnson, L., Olshansky, P.: Securing Tohoku’s future: planning for rebuilding in the first year following the Tohoku-Oki Earthquake and Tsunami. *Earthquake Spectra*, 479–499 (2013). <https://doi.org/10.1193/1.4000119>
  21. Iwasaki, T., Tatsuoka, F., Tokida, K., Yasuda, S.: A practical method for assessing soil liquefaction potential base on case studies at various sites. In: *Proceedings of the Second International Conference on Microzonation for Safer Construction-Research and Application*, pp. 885–896 (1978)


22. Kaistrenko, V., Pinegina, T., Klyachko, M.: Evaluation of tsunami hazard for the Southern Kamchatka coast using historical and paleotsunami data. Underwater ground failures on tsunami generation, modelling, risk and mitigation. In: Yalciner, A.C., Pelinovsky, E., Synolakis, C.E., Okal, E. (eds.) *Submarine Landslides and Tsunamis NATO Science Series: IV. Earth and Environmental Sciences*, vol. 21, pp. 225–235. Kluwer (2003)
23. Kantarzhi, I.G., Akulinin, A.N.: Physical modeling of tsunami waves impact on shore structures. *Fundam. Appl. Hydrophys.* **10**, 83–90 (2017). <https://doi.org/10.7868/S2073667317030078>
24. Kantarzhi, I.G., Gubina, N.A., Gusarov, R.N.: Effects of long waves on coastal hydraulic structures. *Power Technol. Eng.* **55**, 219–222 (2021). <https://doi.org/10.1007/s10749-021-01343-x>
25. Keller, A., Wilson, H.: *An Evaluation of Chemically Related Disasters Using the Bradford Disaster Scale*. Disaster Prevention and Limitation Unit. University of Bradford (1989)
26. Klyachko, M.: Complex Engineering Program of Preparatory Measures on Mitigation of Damage from the Forecasted EQ in Kamchatka, UNDRRO Conference, Moscow (1989)
27. Klyachko, M., Raisman, M.: Medical aspects of disaster preparedness to strong earthquakes on the Kamchatka. *Prehosp. Disaster Med.* **10**(S2), S46–S46 (1995). <https://doi.org/10.1017/S1049023X00501241>
28. Klyachko, M., Koff, G., Polovinchik, J.: Development of Earthquake Disaster Scenarios (EQ DISC) for analysis and management of seismic risk for urbanized areas. In: 1st Egyptian Conference On EQE Cairo, pp. 505–514 (1993)
29. Klyachko, M.: Arguments for earthquake hazard mitigation in the Kamchatka region NATO ASI Series E: Applied Sciences, vol. 271, pp. 215–219. Kluwer (1993). <https://discover.libraryhub.jisc.ac.uk/search?q=Klyachko&rn=11>
30. Klyachko, M.: Scale of disasters. *J. Civil Protect.* **2**, 53–56 (1994a)
31. Klyachko, M.: The lessening of urban vulnerability is a main way to mitigate the disaster. In: *Proceedings of the 9th International Seminar on EQ Prognostics*. San Jose, Costa Rica, pp. 457–460 (1994b)
32. Klyachko, M.: The Scale for Disaster Magnitude Measurement as Applied to EQs. In: *Proceedings of 9th International Seminar on EQ Prognostics*, San Jose, Costa Rica (1994c)
33. Klyachko, M., Klyachko, I.: The DIMAK scale for disaster magnitude measuring in service. In: Housner, G.W., Chung, R.M. (eds.) *Natural Disaster Reduction. Proceedings of Conferences*, pp. 76–77. ASCE, Washington, DC (1996)
34. Klyachko, M., Dzogaz, V.: Preventive seismic strengthening and urban resilience. In: 1st Croatian Conference on Earthquake Engineering – 1CroCEE. Zagreb, 22–24 March (2021). <https://doi.org/10.5592/CO/1CroCEE.2021.118>
35. Klyachko, M.: How to be prepared practically? In: *Proceedings of 4th Asia-Pacific Conference on Disaster Medicine (APCDM-4)*, September 2–4. Sapporo, Japan (1998)
36. Klyachko, M., Uzdin, A.: Peculiarities of soil structure interaction in construction with artificial bases. In: 2st International Conference on Recent Advances in Geotechnical EQ Eng. & Soil Dynamics, St-Louis, March 11–15, vol. 1, pp. 759–763 (1991)
37. Klyachko, M.: Certification of buildings in seismically hazardous areas of Kamchatka region. In: *International Conference 9ECEEE*, Moscow (1990)
38. Klyachko, M., Koff, G., Polovinchik, J.: Development of GIS for analysis and management of the seismic risk on the urban areas. In: Duma, G. (ed.) *Proceedings of the 10th European Conference on Earthquake Engineering*, vol. 2, pp. 1141–1146. Balkema, Rotterdam (1995)
39. Klyachko, M.: The development of GIS, EQ-DISC and DIMAK as the best tools for seismic risk analysis on the urban areas. In: *Proceedings of 5th International Conference on Seismic Zonation*, Qiest-Editions, vol. 1585 vol. 1, pp. 158–165. Presses Academiques, Nantes (1995)
40. Klyachko, M.: Kouznetsova-Izrahmetova I. Estimation and abatement of the urban seismic risk. In: *Proceedings of “Eleventh World Conference on EQE”*. Acapulco. Mexico (1996). [https://www.iitk.ac.in/nicee/wcee/article/11\\_161.PDF](https://www.iitk.ac.in/nicee/wcee/article/11_161.PDF)

41. Klyachko, M., Maksimov, V., Nudner, I., Filkov, V.: On regional standard "Buildings, structures and areas. Safety requirements under tsunami impact". In: 10 U.S. National Conference on Earthquake Engineering Frontiers of Earthquake Engineering July 21–25. Anchorage, Alaska (2014)
42. Kotitsyna, S.S., Kantarzhi, I.G.: Destructions in the port caused by tsunami waves. *Power Technol. Eng.* **55**, 20–25 (2021). <https://doi.org/10.1007/s10749-021-01313-3>
43. Kuprin, A.V., Novakov, A.D., Kantarzhi, I.G., Gubina, N.A.: Local and general scours caused by tsunami waves. *Power Technol. Eng.* **54**, 836–840 (2021). <https://doi.org/10.1007/s10749-021-01296-1>
44. Larionov, V.: Theoretical Basis of Response to Emergencies. Manuel for Students of Military Engineering University (MEU). Military Engineering University, Moscow (1999) (in Russian)
45. Larionov, V., Frolova, N.: Seismic risk assessment and mapping for the Krasnodar region. In: Proceedings of the Conference of VI Russian Conference on EQE (2005)
46. Makhinov, A.N., Kim, V.I., Ostroukhov, A.V., Matveenko, D.V.: Large landslide in the valley of the Bureya River and tsunami in the reservoir of the Bureya hydroelectric power station. In: Vestnik of the Far-East Branch of the Russian Academy of Sciences, vol. 2, pp. 35–44 (2019)
47. Manual 1: Methodical Manual for passportisation of buildings on seismic-prone areas. K.F. DalNIIS, Gosstroy USSR (1987)
48. Manual 2: Methodical Manual «Initial Database for the Design of Construction Structures on Tsunami-Prone Coasts of the Russian Federation», 127 pages. MoC, Moscow (2018). <http://gost.gtsever.ru/Data2/1/4293727/4293727210.pdf>
49. Manual 3: Methodical manual. Design of buildings and structures in tsunami-prone areas, 73 pages. MoC, Moscow (2018). <https://meganorm.ru/Data 2/1/4293730/4293730179.pdf>
50. Maruyama, Y., Yamazaki, F., Matsuzaki, S., Miura, H., Estrada, M.: Evaluation of building damage and tsunami inundation based on satellite images and GIS data following the 2010 Chile earthquake. *Earthquake Spectra*. **28**, 165–178 (2012). <https://doi.org/10.1193/1.4000023>
51. Mori N., Cox D., Yasuda T., Mase H. Overview of the 2011 Tohoku Earthquake Tsunami Damage and  $I_s$  relation to coastal protection along the Sanriku Coast. *Earthquake Spectra*, 2013, 29, 1\_suppl: pp. 127–143. <https://doi.org/10.1193/1.4000118>
52. Nudner, I., Klyachko, M., Maksimov, V., Filkov, V.: About regional standard "Buildings, structures, and areas. safety requirements under tsunami impact". In: Proceedings of 15th World Conference on Earthquake Engineering 2012. Lisbon, Portugal 24–28 September, vol. 11, pp. 8590–8598 (2012). [https://www.iitk.ac.in/nicee/wcee/article/WCEE2012\\_1450.pdf](https://www.iitk.ac.in/nicee/wcee/article/WCEE2012_1450.pdf)
53. Park, H., Cox, D.Y., Barbosa, A.R.: Comparison of inundation depth and momentum flux based fragilities for probabilistic tsunami damage assessment and uncertainty analysis. *Coast. Eng.* **122**, 10–26 (2017)
54. Papadopoulos, G.A., Imamura, F.: A proposal for a new tsunami intensity scale. In: ITS 2001 Proceedings, Number 5-1, pp. 569–577 (2001)
55. Robertson, I., Chock, G., M. EERI, Morla, J.: Structural analysis of selected failures caused by the 27 February 2010 Chile tsunami. *Earthquake Spectra*. **28**, 215–243 (2012). <https://doi.org/10.1193/1.4000035>
56. Ruangrassamee, A., Yanagisawa, H., Foytong, P., Lukkunaprasit, P., Shunichi, K.S., Imamura, F.: Investigation of tsunami-induced damage and fragility of buildings in Thailand after the December 2004 Indian Ocean Tsunami. *Earthquake Spectra*. **22**, 377–401 (2006). <https://doi.org/10.1193/1.2208088>
57. Rutman, Y., Filkov, V.: Determination of the dynamic coefficient under the tsunami bore impact on the protective structure of gravitational type. *Fundam. Appl. Hydrophys.* **10**, 93–97 (2017). <https://doi.org/10.7868/S207366731703008X>
58. Scawthorn, C., Ono, Y., Iemura, H., Ridha, M., Purwanto, B.: Performance of lifelines in Banda Aceh, Indonesia, during the December 2004 great Sumatra earthquake and tsunami. *Earthquake Spectra*. **22**, 511–544 (2006). <https://doi.org/10.1193/1.2206807>
59. Seed, H., Idris, I.: Simplified procedures for evaluating soil li liquefaction potential. *J. Soil Mech. Found. Eng. ASCE*. **97**(SM9), 1249–1273 (1971)

60. Set of Rules 292.1325800.2017 «Buildings and structures on tsunami hazardous areas. Regulations of design». M: Ministry of Construction of Russia, 2017. – 138s
61. SR 38.13330.2012 (Russian national standard). Loads and impacts on hydraulic structures (from wave, ice and ships)
62. Suppasri, A., Charvet, I., Imai, K., Imamura, F.: Fragility curves based on data from the 2011 Tohoku-Oki Tsunami in Ishinomaki City, with discussion of parameters influencing building damage. *Earthquake Spectra*. **31**, 841–868 (2019). <https://doi.org/10.1193/053013EQS138M>
63. Triantafyllou, I., Gogou, M., Mavroulis, S., Lekkas, E., Papadopoulos, G.A., Thravalos, M.: The tsunami caused by the 30 October 2020 Samos (Aegean Sea)  $M_w$  7.0 Earthquake: Hydrodynamic features, source properties and impact assessment from post-event field survey and video records. *J. Mar. Sci. Eng.* **9**, 68 (2021). <https://doi.org/10.3390/jmse9010068>
64. Zayakin Yu. Ya: Kamchatka tsunami catalog.—Obninsk: VNIGMI-MTsD, (1987). 50 p. (in Russian)
65. Zaytsev, A.I., Pelinovsky, E.N., Yalciner, A., Susmoro, H., Prasetya, G., Hidayat, R., Dolgikh, G.I., Dolgikh, S.G., Kurkin, A.A., Dogan, G., Zahibo, N., Pronin, P.I.: Generation of the 2018 tsunami on Sulawesi Island: possible sources. *Dokl. Earth Sci.* **486**, 588–592 (2019a)
66. Zaytsev, A., Kurkin, A., Pelinovsky, E., Yalciner, A.C.: Numerical tsunami model NAMI-DANCE. *Sci. Tsunami Haz.* **38**, 151–168 (2019b)
67. Wood, N., Church, A., Frazier, T., Yamal, B.: Variations in community exposure and sensitivity to tsunami hazards in the state of Hawai'i. In: Geological Survey (U.S.) Scientific Investigations Report. 2007-5208 Report: iv, 38 p (2007)

# Transnational Terrorism as a Threat: Cross-Border Threats



Jake Wright and Silvia D'Amato 

## 1 Introduction

Both as a theoretical area of analysis and as a practical phenomenon, the question of terrorism has grown exponentially in significance over the past few decades and a renewed interest has recently emerged in the policy debate [16]. Overall, strategies and characteristics of this peculiar challenge are no longer solely discussed in academic settings and in strategic documents, but they became an important part of our everyday lexicon in ways that are far more profound than in the past. Among many other issues related to terrorism, in the last few decades, both policymakers and academics have been quite preoccupied with understanding the features and conditions under which terrorist groups are more likely to expand their activities across borders and within different neighbouring countries. Indeed, despite clear domestic claims and histories, many terrorist organisations expand their operational field outside national borders, indicating a general need for a better analysis of these dynamics. Transnationalism, indicating the presence and activities across different countries, might indicate terrorist organisations respond to different strategic needs and actually manifest in different formats and dimensions. However, we are often left wondering what is the exact nature and relevance of this phenomenon. What are the main characteristics of transnational terrorist activities? What are the advantages and potential shortcomings of transnational activism for terrorist groups? And what makes transnational terrorism particularly and uniquely threatening?

In order to provide a refined discussion of the varieties of transnationalism, this chapter reviews and discusses previous research on transnational terrorism and will specifically focus on four dimensions of 'going global', meaning: 'going

---

J. Wright (✉) · S. D'Amato

Institute of Security and Global Affairs, Leiden University, Leiden, The Netherlands

e-mail: [j.n.wright@fgga.leidenuniv.nl](mailto:j.n.wright@fgga.leidenuniv.nl); [s.damato@fgga.leidenuniv.nl](mailto:s.damato@fgga.leidenuniv.nl)



global in movement and targeting', 'going global in communication', 'going global in allegiance', and 'going global in business'. While doing so we emphasise the role played by globalisation in facilitating the transnational turn of many terrorist activities.

At this point, it is also worth clarifying that in this chapter we employ 'terrorism' as umbrella term to include a series of warfare techniques rather than the specific identity of a group or organisation. In fact, despite being one of the most ancient warfare techniques, the label 'terrorist' has featured more heavily in political discourse since the early 2000s, responding to the rise of 'salafist' terror attacks across the Middle East, Gulf, and West Asia, as well as separatist movements [12]. This label has been employed by securitising actors to elicit strong aversion to a group and its goals among the audience [3, 4]. Within the academic debate, 'terrorism' has been largely contested in its objective meaning to underline the political nature of its definition [34] and it is, today, increasingly so also in the general policy discourse. Hence, references will be made to groups using violent means on non-military targets to achieve their political ends. By doing this, we aim to recognise and emphasise that definitions of 'terrorist' are contested and potentially subject to political manipulations without, however, sacrificing its utility as descriptive label.

The chapter is structured as follows: We first set the scene and clarify the definition of terrorism and the general academic discussion on the role of globalisation. We focus then on the four abovementioned dimensions of 'going global' to emphasise key aspects and examples. Finally, we reflect and conclude on the relevance of the study of transnational activities of terrorist organisations and highlight how these might represent a challenge beyond the traditional military battlefield.

## **2 The Story So Far: Terrorism, Transnationality, and Globalisation**

Regardless of their location and specific features, the final goal of terrorist campaigns is to put enough pressure on governments to implement some form of political and/or social change: despite the victims being civilians, terrorists target upwards [17, 36]. Specifically, transnational terrorist groups can be categorised into a few select archetypes. Unlike terrorist attacks per se, transnational terrorism is defined by its cohesion and organisation around a group or, more often, a consistent ideological frame. What makes terrorist organisations transnational can be cross-border supply chains, or a causal timeline between an initial event in one state, and a qualitatively similar event in another state. The former is more indicative of a larger and organised alliance, whereas the latter suggests ideological ties and inspirations from other groups' activities, or through *agitprop*: thus inspiring stochastic terrorism. It is a misnomer to suggest that terrorism was a phenomenon

that was, prior to an arbitrary date of ‘full globalisation’, limited to a nation-state’s borders. Terrorist movements have always moved across borders as well as inspired, supported one another, and learned from each other’s praxis. For instance, the German Revolutions of 1918 were directly inspired and supported by the Bolsheviks who recently took over the Russian Empire in the October Revolution [29], although they lacked the requisite information on tactics used by the Bolsheviks [40]. Despite this, as this chapter aims to demonstrate, globalisation has created new avenues for cooperation across borders, and decentralised command, leading to more resilient networks. Globalisation is interpreted in the literature as an economic, cultural, political, and military phenomenon of accelerated interactions and interconnection [26, 37]. Robertson [71] emphasises the cultural aspect of globalisation, downstream from economic integration, noting the development of a global discourse and culture on ‘the world becom[ing] a single place’ (281–282). Much of this has been fuelled by the internet and its ever-expanding global reach, which interestingly has a comparable timeline to the birth and expansion of Al-Qaeda [51].

Much of the literature on globalisation and its effects on terrorist patterns originate in the first decade of the twenty-first century. Naturally, this was in reaction to the September 11 terrorist attacks and their international character. Literature from this period often pointed to persistent poverty, inequalities within and between states, and oppression against minorities inside a state as conditions for fomenting terrorism [36]. Authors further speculate that globalisation will aggravate these economic inequalities and will engender further anti-Western sentiments in the Global South, leading to them targeting economic institutions that sustains the Western-dominated global market [17, 37]. This is similar to the Marxist organisations targeting business leaders in the 1970s. However, this would disregard the ideological character of white supremacist terrorism as an ideology that appeals to a privileged majority. This would also contradict the premise that oppressed minorities are a fertile ground for building terrorist groups. Overall, authors of this era appear to have over-emphasised the Middle East and North Africa as hostile to the West and uniquely capable of destabilising US hegemony. As the rise in white supremacist terrorist attacks in Germany, New Zealand, the UK, and the United States show, there is a need to zoom the focus out. While this chapter will not depart fully from previous works, it will attempt to recontextualise previous assumptions on globalisation and how terrorist organisations can utilise this interconnectedness for the furtherance of its goals.

Indeed, we focus on transnationality as a multifaceted concept. Transnational terrorism can conjure images of elaborate, multi-stage, multi-actor plots across several regions of the globe, but transnational terrorism can equally apply to recruited foreign fighters relocating to a country to commit a domestic attack. This chapter considers all potential characteristics that make a terrorist organisation transnational and discuss this in relation to the broader phenomenon of globalisation. Specifically, to operationalise globalisation and the transnationalism of terrorist groups, we focus on four aspects of ‘going global’: (a) ‘going global in movement and targeting’, meaning cross-border movement for relocation as well as for implementation of attacks; (b) ‘going global in allegiance’ meaning transnational connections and

supporting activities of different organisations; (c) 'going global in business', meaning global financing and transnational business activities; and (d) 'going global in communication' referring to transnational communication through the Internet and social media, including propaganda purposes.

What emerges is a complex, interconnected network of individuals, businesses, and 'full time' terrorist organisations that are consistently evolving and adapting. Similarly, the countering of this phenomenon is similarly networked and fluid, which will be discussed in the latter half.

## ***2.1 Transnational Terrorism Today: The Ways to 'Going Global'***

### **'Going Global' in Movement and Targeting**

There are tactical and logistical advantages for a group to become transnational, but also challenges in maintaining discipline and political focus. Scholars have therefore tried to identify the conditions for endemic terrorist movements to transfer to another state.

A foundational logic in some part of the literature within International Relations (IR) (see [24]) is that fragile states promote the growth of transnational terrorism. Piazza [46], for instance, shows that there is a disproportionate contribution from 'failed and failing states' to extant transnational terrorism and its operations (p. 483). Although Piazza puts both failed states with failing states in attracting terror, others argue that transnational terrorist organisations prefer to move and operate out of the latter [66]. Overall, terrorist organisations play a delicate balancing act in where they choose to host their operations. Menkhaus [66] finds that terrorist organisations prefer weak state legal systems that allow for effective capture, as opposed to outright lawlessness and complete state failure. This is because an outright failed state encourages the intervention of counterterrorism from the international community with significantly more resources. Degrees of state failure also can affect the types of attacks that can be organised within its territory. George [61] finds that fragile states are more likely to host complex-type attacks—those that involve much more resources, variables, and risks of exposure. However, he also underlines that the fragility of a state does not necessarily align with the nationality of the attacker, seeing as Saudi attackers were overrepresented in transnational terrorist attacks. Instead, fragile states would serve as fertile ground for terror entrepreneurs to create training hubs for aspiring recruits.

While it is safe to say that a globalised system can better facilitate the movement of capital, people, and information without major obstacles, terrorist organisations are limited by their disposable resources and tend to operate inside of regional 'hot spot' neighbourhoods [63]. These neighbourhoods experience, compared to an 'average neighbourhood in the international system', a higher occurrence of terrorist attacks (285). 'Hot spots' are also characterised by the presence of many high-

value targets, porous borders, and weak political institutions to tackle extant terrorist groups. Therefore, there is a noticeable plurality of scholars that view fragile states as breeding grounds or 'safe havens' for transnational terrorist organisations to operate from and move to.

However, part of the literature also warns against some of these conclusions, arguing that some of these observations might be over-essentialised. D'Amato [18] highlights the costs associated with moving terror operations across borders. Without de facto control of territory, as often happens in the so-called 'safe havens', there are physical, social capital, and strategic costs associated with acting transnationally. Therefore, operating abroad might not be a simple and direct consequence of lack of strong institutions, but rather a careful conclusion of a cost-benefit analysis. In the case of Al-Qaeda in the Islamic Maghreb (AQIM) and *Jamā'at Ahl as-Sunnah lid-Da'wah wa'l-Jihād* (colloquially known as Boko Haram), for instance, the overactive and 'hard stick' approach of the Algerian and Nigerian security apparatuses seems to better explain the transnational operations of these organisations.

Overall, insurgent organisations are typically able to entrench themselves among local communities due to the security and services they might provide that the state can (or will) not. When researching transnational terrorist organisations, it is fundamental for researchers to first consider the material circumstances of each region or 'neighbourhood' and what these organisations may offer the population they would otherwise lack.

There is an ongoing division in the literature on what states and demographics are more likely to be targeted in transnational terrorist attacks. Some of the terrorist attacks with the highest fatalities were those targeting the 'far enemy', meaning a foreign demographic and required further complexity than domestic attacks. These are often prescribed in the foundational ideology of the organisation, as was the case with Al-Qaeda and the attack on the World Trade Centre and the Pentagon [22]. However, these attacks can also be in reaction to changing circumstances, and an attempt to internationalise a localised rebellion. In this sense, questions arise as to whether societal differences play a part in what states terrorist groups choose to target and whether a state's integration into the global economic system is correlated to a greater risk of transnational terrorist attacks occurring in its territory. Li and Schaub [35] explore the effects of economic development and integration on the frequency of terrorist attacks in a country. They find that economic integration and development, in fact, reduce the likeliness of a transnational terrorist attack. One of their models showed a 19.3% decrease in the likeliness of experiencing a transnational terrorist attack for every 1% increase in GDP per capita. The implications for this research have been very broad, often seeping into policymaking institutions and think tanks. This would suggest that globalisation, in fact, does *not* help terrorist groups conduct transnational, more elaborate attacks.

Other scholars have argued, however, that wealthier democracies are considered more valuable targets for transnational terrorist organisations, due to their free press and incentive to cover damaging attacks. This is contrasted with authoritarian regimes who are predilected to secrecy and cover-ups to mask inherent instability in

the regime's rule [46]. Moreover, they argue democracies are easier to operate in as a home country and more attractive as an attack destination, because civil society can pressure political apparatuses to respond, an often sought-after goal with terrorist groups [35, 57]. This may be cause for concern for policymakers in democratic regimes and would necessitate stronger transnational counterterrorism measures to identify suspected individuals and frustrate efforts to attack these states.

However, historical analysis of terrorist attacks from 1970 to 2006 suggests that terrorist attacks have been concentrated to specific countries. LaFree et al. [33] found that just 10 countries had been the location for 38% of all terrorist attacks, with 75% of attacks in 32 countries. Carter and Ying [12] directly contradict the conclusion that democracies are more like to be attack destinations. They found no relationship between a state being democratic, and the likeliness of a terrorist attack occurring or being organised on its territory. Instead, using the structural gravitation model, they propose that foreign policy objectives differences better predict attack destinations. It is the 'extreme' relative difference between the home state's foreign policy goals when contrasted to destination's, and their closeness to the United States, which 'attracts' the flow of transnational terrorist attacks. Thus, despite globalisation providing affordable travel opportunities, and facilitating inter-continental connections, terrorist attacks do not appear to have similarly reached across the globe equally. Plümper and Neumayer [47] concur with this position, arguing the level of democracy is related to the power disparity between foreign counterterrorist alliances this finding, but found that regime type has no effect on the coverage of attacks. Insurgent terrorist organisations will, as an intermediate goal, begin to target foreign allies of their home country if this foreign ally is militarily more capable than the home country. This can lead to increased support for the group among the domestic base, due to the perceived illegitimacy of the foreign troops on the country's soil. Carter and Ying [12] liken organisations to businesses, emphasising the hierarchy of political goals and balancing their associated costs, similar to D'Amato [18] above. These findings have considerable repercussions for the broader discussion on the linkage between democracy, security, and economic prosperity. It is a discussion on which many assumptions are made about the United States, its allies, and its position in the world.

There are also debates on the effects that ideology plays on terrorist organisations going transnational in their targeting. Due to the wider exposure Islamic fundamentalist attacks have been given, the question whether these groups conduct more, and deadlier attacks than non-fundamentalist groups, has arisen. Klein [31] investigated the hypothesis that Islamic fundamentalist attacks are both more likely to be transnational and deadlier, on the basis that religious justifications allow for the easier construction of a transnational 'other'. He found, excluding the Kenyan 1998 embassy bombing and 9/11 as outliers, that transnational Islamic fundamentalist attacks did not create higher death counts than others. Saying that attacks across borders typically resulted in more deaths, potentially due to their increased complexity and scope. Carter and Ying [12] also demonstrate that Islamic fundamentalist groups are less likely to target non-Islamic states, countering the

highly reductive conclusion of Huntington [65] and his belief in ‘bloody borders’ between ‘Islamic’ and ‘non-Islamic’ civilisations.

Transnational terrorist attacks, despite *potentially* being organised anywhere around the world, it is clear they are clustered in a very limited number of countries and are motivated by political goals and antagonisms. Thus, it raises questions on where resources should be allocated to tackle these transnational actions most effectively. Policymakers should keep in mind the non-trivial costs transnational terrorist organisations incur when organising, and balance that with the potential goals it can achieve with a successful attack.

### ‘Going Global’ in Allegiance

Terrorist groups form alliances with each other to exchange best practices, technical knowledge, or receive needed supplies. Horowitz and Potter [28] found that, like cooperating states and businesses, terrorist groups partner up for mutual benefit. Among the effects of these alliances is the improved efficacy of their attacks—more elaborate attacks can be executed, and fatalities are increased. Some provided examples include the partnership between the Provisional IRA (PIRA) and the Colombia FARC, where it is speculated a series of successful assaults against the Colombian government were conducted by mortar inspired by the PIRA homegrown mortar device. The PFLP-Special Operations Group (SOG) hosted the Maoist organisation, the Japanese Red Army, and conducted an attack on the Lod Airport in Israel together. The trade here was more fighters for the PFLP-SOG to execute its attacks, in exchange for passing on experience, techniques, and knowledge to the Japanese Red Army to take back to their region.

Not all alliances between groups are equally effective, they appear to operate on a core-periphery model. Groups with renowned reputations for being efficient and deadly seek alliances with similarly renowned organisations (2012). They also tend to have multiple alliances operating at once, with a higher degree of alliance depth, which align with higher predicted fatalities per attack. Thus, these organisations benefit the most from allying with sympathetic groups. Likewise, allying with less renowned organisations provides little benefit to either party [28]. However, there are so-called ‘alliance hubs’, organisations renowned for allying with several groups simultaneously and bridge collaboration between disparate ones [6]. Thus, alliance networks consist of a ‘core’ of organisations with similar political goals that collaborate with others often, and a periphery of smaller, satellite organisations that are perceived as less successful and smaller scale; there is little incentive for organisations to collaborate with the latter. Hub organisations appeal to smaller terrorist groups with their access to needed knowledge and resources that they usually would have no access to. Possession of territory and displays of capabilities act as advertisements for ideologically sympathetic groups to pledge allegiance to these hubs. As this group is combated, and loses access to much of its territory and resources, its alliance network begins to dwindle, and only attracts less capable

groups [6]. These less capable groups are seen as less bother than they are worth and thus still do not attract former alliance hub organisations. This is the paradoxical situation the Islamic State ended up in after it lost most of its territory in 2017. Moderately successful organisations like Boko Haram ceased their allegiance to the Islamic State, and very few organisations (mainly in South Asia) wished to join the network [6].

When do terrorist groups ally with each other, and what are the consistent explanatory factors for these alliances? There are a number of factors that play into forming transnational alliances aside from consistent ideologies. Bacon [6] underlines that the first step is to consider the organisations' primary needs in seeking an alliance with hub organisations. These are as followed: (a) training and operational assistance, (b) sanctuary or protection from adversary or counterterrorism efforts, and (c) mobilisation of needed resources.

Yet, there are also obvious risks for organisations that ally together. Being clandestine in nature, survival of the cadre is always at the top of their priorities [5]. Alliances can jeopardise the survival of a group and its political mission; infiltration by an adversary is a particular concern [6]. As organisations exist for longer periods of time, the leadership becomes predominantly concerned with forcing allegiance, maintaining group solidarity, and preventing factionalism, rather than the achievement of their political goals [6, 15]. This undoubtedly hampers the efficacy and flexibility of these alliances and their willingness to risk it all for a little more.

The characteristics of organisations, and their objectives, also affect the likeliness of them forming alliances. Phillips' [70] survey of international alliances formed between 1987 and 2005 shows that groups motivated by religion are significantly more likely to form international alliances, as are groups sponsored by a state such as Iran (p. 1011). Group membership also plays a part in forming alliances. As stated above, small-size groups do not attract cooperation from more advanced, larger groups, as there is little to gain for them. However, groups with a 'moderate' membership (100–900 members) occupy the 'goldilocks zone', and attract similarly sized groups to assist in attacks on a more powerful enemy: such as a rival group, or a hostile state. Thus, it is important to understand that alliances do not necessarily improve terrorists' capabilities to achieve their goals, rather it is a carefully calculated weighing of costs and benefits.

Overall, across different world regions, insurgent and terrorist organisations use alliances to receive support as well as to increase their visibility and therefore their perceived power within and across their supporting base as well as in the eyes of their opponents [64]. The way these connections and supporting practices are implemented might vary but it is a very common feature and important aspect of terrorist campaigns that academics and policymakers alike should keep analysing.



## ‘Going Global’ in Business

Monetary support to terrorism takes several forms, facilitated and obfuscated due to decentralisation and globalisation. Remittances have historically, and continue to be, a primary source of income for clandestine groups. Mascarenhas and Sandler [38] found a strong linkage between a national of a ‘failed state’ with an insurgency sending remittances back home, and the likelihood of a terrorist attack occurring.

The financing networks of terrorist organisations are eclectic and flexible. Conventional electronic transfers directly to suspects leave a potentially traceable payment trail, and financial regulations such as know-your-customer (KYC) protocols can help prevent this. However, digital transactions are not sufficiently regulated to prevent these transfers from being completed [2] and suspects are often convicted after attacks have been successfully funded [52]. Indeed, the considerable number of simultaneous global transactions would make this difficult to identify in one occasion [55]. Alongside remittances and transfers, terrorist organisations might establish charitable foundations to have a public-facing entity that can solicit donations for a sympathetic cause, and recruit new volunteers for their cause. The Irish-American charity Noraid, helped provide needed funds to the Provisional Irish Republican Army’s families, while the diaspora helped arm active militants [58]. Al-Qaeda and its use of overseas charities received significant attention after 9/11, with the Saudi al Haramain Islamic Foundation operating in Bosnia and Herzegovina, or the Global Relief Foundation in Pennsylvania. Charity personnel thought to be sympathetic to Osama Bin Laden’s cause were named a considerable contributor to Al-Qaeda’s bottom line in the run up before 9/11 [48]. Accusations of this nature can also be highly politically motivated, however. Several organisations in the Netherlands have campaigned for the defunding of Palestinian human rights NGOs on the unsubstantiated grounds that they are monetarily supporting proscribed terrorist groups [21].

Another often cited means to transfer money with relative security, for transnational terrorist groups operating in the Sahel, West and Central Asia, is the ‘*hawala*’ system. *Hawala* is an informal means of moving money across borders using trusted partners and a network of debt and repayment. It can be considered a physical version of Western Union [8]. There is very little paper trail, and *hawaladars* (money ‘movers’) use unrelated business accounts to avoid suspicion that large deposits might incur [11]. *Hawala* is used primarily as a method to remit money abroad at a comparatively lower cost, and with less regulatory scrutiny, than other platforms. The degree of *hawaladar* involvement in more serious illicit activity has not been fully surveyed, and it would be fallacious to tar the entire practice as heavily synonymous with terrorist financing [50]. Al-Qaeda’s use of *hawala* for its funding of attacks is also heavily disputed: Some claim it sourced most of its money through *hawala* networks before 9/11 [48], whereas others argue there is no evidence for this and is used to stigmatise this informal remittance system [42, 56]. This feat notwithstanding, the network can collapse should just one of the *hawaladars* be compromised, as was the case of the Al-Qaeda *hawala* network after 9/11 [48].



A recent way to avoid crackdowns on front organisations has been the use of pseudonymous digital currencies, also known as cryptocurrencies. Cryptocurrencies use cryptography to encrypt the details (sender and recipient) of a transaction, but have a decentralised public ledger to record all transactions made. There is a critical flaw with many conventional cryptocurrencies, however: once they are 'cashed-out' into fiat currencies, the transaction can be traceable [20]. Additionally, the wallet address of individuals and organisations can be traceable through forensic analysis of their transactions. Once identified, transactions of associated accounts can be publicised through social media (see Neonazi BTC Tracker for an example). All of these transactions are publicly available, due to the nature of the blockchain. There are ways to subvert these limitations, such as using fully anonymous coins like Monero or Zcash, that hide transaction information from both parties and the blockchain. Another is to 'mix' the cryptocurrency with other transactions and currencies to hide the payer and the recipient [60]. Methods to counteract terrorist financing through cryptocurrencies is beyond the scope and technical focus of this chapter, but it is important to highlight the unfolding and changing funding landscape for transnational terrorist organisations.

In many instances, such a focus on the use of technologies by terrorist organisations for financing purposes builds on a much broader discussion on the distinction between groups that employ violence to advance political goals (often referred to as an insurgency), and those that employ it for monetary gain (more properly referred to as criminality) [23, 27, 49]. Without entering the details of such debate, we find interesting to point to studies such as Palma [69] that problematise this dichotomy. Terrorist groups, it is found, require consistent funding, and being made illegal as an organisation drastically lowers the cost of engaging in illegal activities, the most profitable being the narcotics trade. Indeed, by negotiating with growers of narcotic products (coca leaves, opium, etc.) and providing security as well as a bulk buyer of their products, the terrorist organisation can gain a legitimate foothold in these communities [14]. In this sense, we highlight, local and global business of many groups and organisations is not necessarily about economic gain but rather about building legitimacy and increasing political control.

### **'Going Global' in Communication**

Communications across borders remain a keystone part of transnational terrorism for recruitment, inspiration, and messages of solidarity between groups. As Klein [31] reminds us, terrorist attacks are messages in, and themselves, a 'propaganda of the deed', to quote Kropotkin [32]. Through messaging and online comments, groups often react to successful attacks, or military victories, expressing support or taking specific positions on particular matters or actions. For instance, jihadist organisations worldwide congratulated the Taliban for taking control of the Afghanistan government, Hayat Tahrir al-Sham organised parades in Idlib to celebrate [1]. Conversely, terrorist groups can also publicly distance themselves from others in the same field with statements. The Popular Front for the Liberation of

Palestine (PFLP) distanced itself from the PFLP-General Command after it attacked the Palestinian Yarmouk camp in Syria [45]. Online far-right communities often collaborate to organise in-person events to facilitate networking and interaction across borders [19]. Overall, however, the primary goal of transnational online communication is gaining sympathies and new recruits [9].

Distinct from structurally decentralised, but ideologically compatible terrorist groups, globalisation provides a multitude of opportunities for all actors (both individual and organisation) to disseminate *agitprop* to susceptible audiences. Social media and messaging platforms are host to a number of small-to-medium-sized like-minded communities that form an echo-chamber for its members to reaffirm their political beliefs. These are effective platforms for sharing ideologically sympathetic and riling content among its members but, perhaps out of fear of censorship or reprisal, instructions for how to exercise these ideological goals is scarce [72]. Contrary to expectation, though, Guhl and Davey [62] suggest these looser and more decentralised networks of sympathisers can be similarly effective in inspiring violent action. Wakeford and Smith [54], however, argue there are limits to proving causation in assessing the efficacy of online radicalisation. It is unclear to what degree regular consumers of online *agitprop* are converted to offline terrorists. They use the phenomenon of ‘clicktivist’ or ‘slacktivist’ to argue there is no such ‘slippery slope’ (158). Despite this, the authors recognise the influence the internet had on the Manchester bomber in 2017. Thus, setting aside the efficacy of online communications, there are several spectacular terrorist attacks that can be attributed to online radicalisation, altering the modern, common conception of transnational terrorist groups. We find interesting to focus specifically on the use of digital communication for recruitment and agitation.

Alongside the 2017 Manchester bombing, the Christchurch shooting, and the ‘memeification’ of this reprehensible attack has demonstrated the power that online communications can have on susceptible candidates for ‘lone wolf’, stochastic attacks. This attack, committed by Brenton Tarrant, was livestreamed in its entirety on Facebook Live and viewed thousands of times. Before the attack commenced, Tarrant published his manifesto on the far-right 8chan/pol/internet message board. Although not unique in any of its composite elements, the Christchurch shooting was the most successful streamed mass shooting of all time and led to Tarrant, despite his incarceration, becoming a commemorated figure head of the online far-right. As the shooting was unfolding, and even now, the footage featured in images, flashy promotional videos for far-right online communities, and Tarrant’s manifesto has been cited in other mass shootings (such as in the El Paso shooter’s manifesto).

Much of the work on the communication of transnational terrorist organisations has primarily used jihadist extremist groups as case studies, a limitation that Conway [13] argues should be addressed in future scholarship. Zelin [59] demarcates four phases in jihadist communication, ending in modern online communication. The first phase used post and physical media such as magazines to advertise the organisation’s mission and activities, it then transitioned into the second phase of

Web 1.0 websites and the networking of sympathetic terrorist media groups. The first two phases required the outlay of capital and a front face for the organisation. The third phase was the introduction of Web 2.0 and the relocation of propaganda to Internet forums and social media sites. The fourth phase involves the co-creation of propaganda by members of the terrorist organisation and sympathisers alike, using social media sites and 'Software as a Service' to minimise costs for disseminating their message. As time has gone on, then, transnational communication for terrorist organisations has become exponentially cheaper and decentralised. Although other ideologies may have different initial phases, the end point of using Web 2.0 social media sites, such as Telegram, Gab, Twitter, or Facebook, is the same. As extremist movements decentralise, anonymous, dynamic, and quickly replaceable online platforms for disseminating *agitprop* (agitation propaganda) are the natural response to harsher counterterrorist efforts. Creating an echo-chamber or 'pipeline' for radicalising a susceptible demographic is essentially free, effective in affirming victim narratives [67], and quickly expands its consumer base. The existence of an actual 'slippery slope' from consuming extremist content to committing a terrorist attack is spurious, but the consumption alone affects how the audience interprets social relations. Using the examples of ISIS, extremist propaganda involves the simple dichotomisation of society [68] – the virtuous and pious (those who will comply with the primary message of the organisation) versus the 'enemy' (anyone who would resist it, regardless of how much). This mentally restructures the consumers' outlook and colours how they interpret societal relations ([25, 39, 53]). The consumer morally justifies their actions; minimises, ignores, or misconstrues consequences of reprehensible behaviour; and blames the victim for this behaviour [7].

Mainstream social media sites (Twitter, Facebook, Instagram, YouTube, etc.) have attempted to clamp down on extremist content by banning far-right content creators. However, the migration of these creators to alternative sites with slacker moderation, or sympathetic moderators, only heightens the 'tunnel vision' consumers of this propaganda experience, because they are drawn to a site with higher concentration of extremist content.

How organisations recruit, organise, and inspire susceptible sympathisers online is an important part of understanding transnational terrorism. Unlike the other transnational conduct described above, distributing *agitprop* and attracting a susceptible audience is effectively cost-and-risk-free. Moreover, many of the most spectacular and scarring attacks in Europe, North American, and New Zealand were perpetrated by 'lone wolf' regular consumers of this propaganda. Finally, it is very difficult to fully ban this propaganda. Accounts that are taken down are very quickly brought back up with the same content as before, or moved to more sympathetic platforms. The method of communicating extreme messages also rapidly changes, requiring moderation staff to stay up-to-date constantly with the latest insinuations and inside 'jokes' of those communities.

### 3 Transnational Terrorism, Responses, and Remaining Challenges: Final Remarks and Conclusions

Transnationality today is a key, generalised and undeniable feature of many terrorist organisations. Across different world regions, political settings, and ideologies, we find groups implementing or taking advantage of transnational possibilities, especially facilitated by the dynamics of globalisation. As we have seen, the question for many policymakers and academics is how to respond to this. Indeed, the possibility to operate, communicate, and organise across borders presents some advantages to terrorist organisations and it challenges states' security apparatuses, still largely dependent on national capabilities and operative structures [30]. One of the main issues for states concerns the realisation that the peculiar transnational nature of terrorism makes a traditional counterterrorism military strategy far less effective. Indeed, current forms of transnational terrorism do not represent a security challenge for their operative strategies on the ground but also in light of their facilitated communication and funding activities across the globe. The realisation of these shortcomings pushed a large part of the policy world to focus on a problem-solving approach based on cooperation and creation of counterterrorism networks [43]. The idea is, as summarised by Nye [41] two decades ago, that 'the best response to transnational terrorist networks is networks of cooperating government agencies'. As mentioned, cooperation on solely military terms did not prove to be particularly effective in solving the actual cause of transnationalism and therefore the overall problem in mid-long term. Crenshaw ([16]: 19), for instance, has recently underlined how 'military force can destroy a terrorist base, remove key leaders, and disrupt operations in the short term, but it may increase local instability and motivate transnational terrorist attacks in the longer term. An added complication is that when foreign intervention intended to retaliate for terrorism or defend a threatened government precipitates more terrorism and internal disorder, the third party finds it hard to withdraw from its commitment because the local partner cannot provide security. IS is already regrouping in Syria and Iraq following the abrupt withdrawal of US troops in October 2019'.

Accordingly, there has been an attempt to respond along different lines, especially when considering terrorist transnational business and communication, reinforcing dynamics of regionalisation and regional governance where security, political but also economic interactions between different states are redesigned [44]. Border-spanning discourses, institutions, and agencies are generated as new social spaces to facilitate cross-border cooperation as well as information flow and sharing with preventive but also prosecuting purposes across the globe [10]. Nonetheless, cooperation in these fields also remains challenging. It is complex to sustain and generally significantly slower than the evolution of the nature and the tools employed by the threat they intend to address as it necessitates constant disclosure, convergence on bureaucratic practices, and a commitment in information sharing.

Overall, this chapter aimed at addressing the main dimensions of transnationalism in order to discuss the varieties of features of this threat and the challenges

it poses. We discussed, in particular, transnationalism over four dimensions indicating different ways to cross-national borders, meaning movement and targeting, allegiance, business, and communication. Across these four dimensions, we have seen how the 'global' could be used in order to increase material and ideological support as well as a facilitator for economic interests and communicative strategies. On a conclusive note, what seems fair to argue is that the challenges posed by transnationalism terrorism do not only concern the characteristics of the threat itself but also the characteristics and difficulties related to many states' structures as well as the features of the international system.

## References

1. Al-Qaeda-linked groups in Syria, Yemen welcome Taliban victory. *The Arab Weekly*. <https://theArabweekly.com/al-qaeda-linked-groups-syria-yemen-welcome-taliban-victory> (2021, August 20)
2. Ashley, S.P.: The future of terrorist financing: fighting terrorist financing in the digital age. *Penn State J. Int. Aff.* (2012). [https://psujia.files.wordpress.com/2012/04/terrorist\\_financing\\_final1.pdf](https://psujia.files.wordpress.com/2012/04/terrorist_financing_final1.pdf)
3. Baele, S., Boyd, K., Coan, T.: Lethal images: analyzing extremist visual propaganda from IS and beyond. *J. Glob. Secur. Stud.* **5**(4), 634–657 (2019a)
4. Baele, S., Boyd, K., Coan, T.: What does the "terrorist" label really do? Measuring and explaining the effects of the "terrorist" and "Islamist" categories. *Stud. Conflict Terror.* **42**(5), 520–540 (2019b)
5. Bacon, T.: Hurdles to international terrorist alliances: Lessons from Al Qaeda's experience. *Terror. Polit. Violence.* **29**(1), 79–101 (2017). <https://doi.org/10.1080/09546553.2014.993466>
6. Bacon, T.: *Why Terrorist Groups Form Alliances*. University of Pennsylvania Press (2018)
7. Bandura, A.: Selective moral disengagement in the exercise of moral agency. *J. Moral Educ.* **31**(2), 101–119 (2002)
8. Biswas, B., Sana, A.K.: Issues in terrorism financing: an analysis. In: Das, R. (ed.) *The Impact of Global Terrorism on Economic and Political Development: Afro-Asian Perspectives*. Emerald Publishing Limited (2019)
9. Brown, K.E., Pearson, E.: Social media, the online environment and terrorism. In: Andrew, S. (ed.) *Routledge Handbook of Terrorism and Counterterrorism*. Routledge (2018)
10. Brunet-Jailly, E.: Cross-border cooperation: a global overview. *Alternatives.* **47**(1), 3–17 (2022)
11. Burr, J.M., Collins, R.O.: *Alms for Jihad*. Cambridge University Press (2006)
12. Carter, D.B., Ying, L.: The gravity of transnational terrorism. *J. Confl. Resolut.* **65**(4), 813–849 (2021)
13. Conway, M.: Determining the role of the internet in violent extremism and terrorism: six suggestions for progressing research. *Stud. Conflict Terror.* **40**(1), 77–98 (2017)
14. Cornell, S.E.: The interaction of narcotics and conflict. *J. Peace Res.* **42**(6), 751–760 (2005)
15. Crenshaw, M.: An organizational political approach to the analysis of political terrorism. *Orbis.* **29**(3), 465–489 (1985)
16. Crenshaw, M.: Rethinking transnational terrorism: an integrated approach. In: *Peaceworks*, p. 158. United States Institute of Peace, Washington (2020)
17. Cronin, A.K.: Behind the curve: globalization and international terrorism. *Int. Secur.* **27**(3), 30–58 (2002)
18. D'Amato, S.: Terrorist going transnational: rethinking the role of states in the case of AQIM and Boko Haram. *Crit. Stud. Terror.* **11**, 151 (2017)

19. Davey, J., Ebener, J.: *The Fringe Insurgency. Connectivity, Convergence and Mainstreaming of the Extreme Right*. Institute for Strategic Dialogue (2017). <http://www.isdglobal.org/wp-content/uploads/2017/10/The-Fringe-Insurgency-221017.pdf>
20. Entenmann, E., van den Berg, W.: *Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?* ICCT (2018). <https://icct.nl/publication/terrorist-financing-and-virtual-currencies-different-sides-of-the-same-bitcoin/>
21. European Legal Support Center: *Monitoring Report: The Attempt to Chill Palestinian Rights Advocacy in the Netherlands*. European Legal Support Center (2021). <https://cms.elsc.support/wp-content/uploads/2021/10/ELSC-The-Attempt-to-Chill-Palestinian-Rights-Advocacy-in-the-Netherlands.pdf>
22. Gerges, F.A.: *The Far Enemy: why Jihad Went Global*. Cambridge University Press (2005)
23. Gray, C.: *War, Peace and International Relations: an Introduction to Strategic History*. Routledge (2007)
24. Grimm, S., Lemay-Hébert, N., Nay, O.: “Fragile states”: introducing a political concept. *Third World Q.* **35**(2), 197–209 (2014)
25. Harlow, S.: Social media and social movements: Facebook and an online Guatemalan justice movement that moved offline. *New Media Soc.* **14**(2), 225–243 (2012)
26. Held, D., McGrew, A., Goldblatt, D., Perraton, J.: *Global Transformations: Politics, Economics and Culture*. Polity (1999)
27. Hoffman, B.: *Inside Terrorism*. Columbia University Press (2006)
28. Horowitz, M.C., Potter, P.B.K.: Allying to kill: Terrorist intergroup cooperation and the consequences for lethality. *J. Confl. Resolut.* **58**(2), 199–225 (2012)
29. Jones, M.: *Founding Weimar: Violence and the German Revolution of 1918–1919*. Cambridge University Press (2016)
30. Kirshner, J.: *Globalization and National Security*. Routledge (2013)
31. Klein, G.: Ideology Isn’t everything: transnational terrorism, recruitment incentives, and attack casualties. *Terror. Polit. Violence.* **28**(5), 868–887 (2016)
32. Kropotkin, P.: *Kropotkin’s Revolutionary Pamphlets: A Collection of Writings*. Dover Publications (1970)
33. LaFree, G., Morris, N.A., Dugan, L.: Cross-National Patterns of terrorism – comparing trajectories for total attributed and fatal attacks, 1970–2006. *Br. J. Criminol.* **50**, 622–649 (2010)
34. Jackson, R., Pisiou, D. (eds.): *Contemporary Debates on Terrorism*. Routledge, London (2018)
35. Li, Q., Schaub, D.: Economic globalization and transnational terrorism. *J. Confl. Resolut.* **48**(2), 230–258 (2004)
36. Lia, B.: *Globalisation and the Future of Terrorism: Patterns and Predictions*. Routledge (2005)
37. Lutz, B.J., Lutz, J.M.: Globalisation and terrorism in the Middle East. *Perspect. Terror.* **9**(5), 27–46 (2015)
38. Mascarenhas, R., Sandler, T.: Remittances and terrorism: a global analysis. *Defence Peace Econ.* **25**(4), 331–347 (2014). <https://doi.org/10.1080/10242694.2013.824676>
39. McGarty, C., Thomas, E., Lala, G., Smith, L., Bliuc, A.-M.: New technologies, new identities, and the growth of mass opposition in the Arab spring. *Polit. Psychol.* **35**(6), 725–740 (2014)
40. Mitchell, A.: *Revolution in Bavaria, 1918–1919: the Eisner Regime and the Soviet Republic*. Princeton University Press (1965)
41. Nye, J.S.: U.S. Power and strategy after Iraq. *Foreign Aff.* **82**(4), 60–73 (2003)
42. Passas, N.: Hawala and other informal value transfer systems: how to regulate them. *Risk Manag.* **5**, 49–59 (2003)
43. Perlinger, A.: Terrorism networks. In: Victor, J.N., Montgomery, A.H., Lubell, M. (eds.) *The Oxford Handbook of Political Networks*. Oxford University Press (2017)
44. Perkman, M., Sum, N.L. (eds.): *Globalization. Palgrave Macmillan, Regionalization and Cross-Border Regions* (2002)
45. PFLP on Defense in Gaza Over Ties to Assad: Al-Monitor. <https://www.al-monitor.com/originals/2012/al-monitor/pflp-on-defense-in-gaza.html> (2012, December 28)

46. Piazza, J.A.: Incubators of terror: do failed and failing states promote transnational terrorism? *Int. Stud. Q.* **52**, 469–488 (2008)
47. Plümper, T., Neumayer, E.: The friend of my enemy is my enemy: international alliances and international terrorism. *Eur J Polit Res.* **49**, 75–96 (2010)
48. Roth, J., Greenberg, D., Wille, G.: Monograph on Terrorist Financing. National Commission on Terrorist Attacks Upon the United States (2004). [https://govinfo.library.unt.edu/911/staff\\_statements/911\\_TerrFin\\_Monograph.pdf](https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf)
49. Schmitt, C.: *Theory of the Partisan: A Commentary/Remark on the Concept of the Political*. Michigan State University (1963)
50. Soudjin, M.: Hawala and money laundering: potential use of red flags for persons offering Hawala services. *Eur. J. Crim. Policy Res.* **21**, 257–274 (2015)
51. Stapley, L.: *Globalization and Terrorism: Death of a Way of Life*. Routledge/Taylor & Francis Group (2006)
52. Teichmann, F., Falker, M.C.: Terrorist financing via money transfer systems. *Eur. J. Crime Crim. Law Crim. Justice.* **29**, 103–126 (2021)
53. Thomas, E., McGarty, C., Lala, G., Stuart, A., Hall, L., Goddard, A.: Whatever happened to Kony 2012? Understanding a global internet phenomenon as an emergent social identity. *Eur. J. Soc. Psychol.* **45**, 356–367 (2015)
54. Wakeford, L., Smith, L.: Islamic state's propaganda and social media. In: Baele, S., Boyd, K., Coan, T. (eds.) *ISIS Propaganda: A Full Spectrum Extremist Message*. Oxford University Press, Oxford (2020)
55. Weintraub, S.: Disrupting the financing of terrorism. *Wash. Q.* **25**(1), 53–60 (2002)
56. Viles, T.: Hawala, hysteria and hegemony. *J. Money Laundering Control.* **11**(1), 25–33 (2008)
57. Young, J.K., Findley, M.G.: Promise and pitfalls of terrorism research. *Int. Stud. Rev.* **13**(3), 411–431 (2011)
58. Zach, D.A.: 'It was networking, all networking': the Irish republican movement's survival in Cold War America. *J. Ethn. Migr. Stud.* **47**, 2218–2236 (2018)
59. Zelin, A.: *The State of Global Jihad Online: A Qualitative, Quantitative, and Cross Lingual Analysis*. New America Foundation (2013)
60. Ziegeldorf, J., Matzutt, H., Henze, R., Grossmann, M., Wehrle, F., K.: Secure and anonymous decentralized bitcoin mixing. *Futur. Gener. Comput. Syst.* **80**, 448–466 (2018)
61. George, J.: State failure and transnational terrorism: an empirical analysis. *J. Confl. Resolut.* **62**(3), 471–495 (2018)
62. Guhl, J., Davey, J.: *A Safe Space To Hate: White Supremacist Mobilisation on Telegram*. ISD Global (2020). <https://www.isdglobal.org/wp-content/uploads/2020/06/A-Safe-Space-to-Hate2.pdf>
63. Braithwaite, A., Li, Q.: Transnational terrorism hot spots: identification and impact evaluation. *Confl. Manag. Peace Sci.* **24**(4), 281–296 (2007)
64. Hansen, S.J.: 'Forever wars'? Patterns of diffusion and consolidation of Jihadism in Africa. *Small Wars Insurgencies.* **33**(3), 409–436 (2021)
65. Huntington, S.: *Clash of Civilizations and the Remaking of World Order*. Simon & Schuster (1996)
66. Menkhaus, K.: Quasi-States, Nation-Building, and Terrorist Safe Havens. *J. Confl. Stud.* **23**(2), 7–23 (2003)
67. Marcks, H., Pawelz, J.: From myths of victimhood to fantasies of violence. How far-right narratives of imperilment work. *Terror. Polit. Violence.* **34**(7), 1415–1432 (2020)
68. McCauley, C., Moskalenko, S.: *Friction: How Radicalization Happens to Them and Us*. Oxford University Press (2011)
69. Palma, O.: Transnational networks of insurgency and crime: explaining the spread of commercial insurgencies beyond state borders. *Small Wars & Insurgencies.* **26**(3), 476–496 (2015)
70. Phillips, B.J.: Terrorist group rivalries and alliances: testing competing explanations. *Stud. Confl. Terror.* **42**(11), 997–1019 (2019)
71. Robertson, R.: *Globalization: Social Theory and Global Culture*. Sage (1992)
72. Walther, S., McCoy, A.: US extremism on telegram: fueling disinformation, conspiracy theories, and accelerationism. *Perspect. Terror.* **15**(2), 100–124 (2021)



# Resilience Against Hybrid Threats: Empowered by Emerging Technologies: A Study Based on Russian Invasion of Ukraine



Scott Jasper

## 1 Introduction

Early on the morning of January 14, 2022, a cyberattack defaced more than 70 Ukrainian government websites with threatening messages written in multiple languages [1]. The next day, Microsoft revealed that destructive wiper malware, disguised to look like ransomware but absent a recovery mechanism, was concurrently emplaced in dozens of computers at Ukrainian government agencies [2]. The Ukrainian Ministry of Digital Development stated “all evidence indicates that Russia is behind the cyberattack. Moscow continues to wage a hybrid war and is actively building up its forces in the information and cyberspaces.” [3] National Defense University researcher Frank Hoffman, the originator of the term, has called hybrid war “a merger of different modes and means of war.” [4] Ever since the unlawful seizure of Crimea in 2014, Russia has used a blend of military, economic, and other measures to pull Ukraine closer into its sphere of interest [5]. The fused measures are meant to destabilize Ukraine, which is seeking to integrate with the West. As part of the Russian hybrid campaign, Ukraine suffered a series of cyberattacks that have knocked out power, frozen supermarket registers, and forced authorities to prop up their currency after bank IT systems crashed [6]. The dual cyber incidents came during the threat of an imminent invasion by over 160,000 Russian troops and equipment near the border of Ukraine, accompanied by further cyberattacks [7].

Moscow leveraged military intimidation to demand that the North Atlantic Treaty Organization (NATO) halt any further enlargement, bar Ukraine from joining, and pull back forces and weapons from eastern European countries [8]. Moscow tried

---

S. Jasper (✉)

Naval Postgraduate School, National Security Affairs, Carmel, CA, USA

e-mail: [sejasper@nps.edu](mailto:sejasper@nps.edu)



to use energy as a weapon to stymie a unified European position of defiance, since Russia provides about 40% of natural gas for the 27-country bloc. Germany in particular is highly reliant on Russia for half of its gas imports and was hesitant to embrace strict U.S.-led economic penalties should Russia invade. After meeting with President Biden, the new German Chancellor Olaf Scholz refused to publicly commit to stop the recently finished Russian-built Nord Stream 2 natural gas pipeline [9]. Meanwhile, Berlin faced criticism for not exporting lethal weapons to Kyiv at the time and blocking fellow NATO ally Estonia from sending German-origin D-30 howitzers, citing arms export policies for conflict zones [10]. Diplomatic maneuvers and energy coercion are non-military methods for influence, while military forces provide the means for pressure by force. The Russian military was rebuilt after the Soviet collapse, with more tanks, rocket launchers, self-propelled guns, and towed artillery than any other nation [11]. It is armed with an array of conventional missiles and new hypersonic missiles, like Avangard, Kinzhal, and Zircon. On February 24, 2022, Russian President Putin said on state television “he had been left with no choice” but to launch “a special military operation” to demilitarize Ukraine [12].

A year earlier, at the 2021, Brussels Summit, the Heads of State and Government of the thirty NATO Allies, stated in their Communique that “we are increasingly confronted by cyber, hybrid, and other asymmetric threats, including disinformation campaigns, and by the malicious use of ever-more sophisticated emerging and disruptive technologies.” [13] Russia embodies this threat as evident by a range of hybrid actions taken to undermine NATO and partner nation stability and security. The 2021 Communique identifies that besides military activities, hybrid actions include “attempted interference in Allied elections and democratic processes; political and economic pressure and intimidation; widespread disinformation campaigns; [and] malicious cyber activities.” In addition, Russia has embraced ever-more sophisticated emerging technologies, such as hypersonics to surpass the United States in development of so-called invincible weapons. These technologies embolden and empower Moscow to be more assertive on the world stage as it strives to resume its status as a great power. This chapter will start by describing definitions of a hybrid threat, the origin of the idea, and the conceptual basis in the context of Russian applications. It will then outline US and NATO interpretations and classifications of emerging technologies, with subsections devoted to Russian development and employment of three select areas. Finally, the chapter will examine resilience, seen in the Ukrainian response to Russian aggression.

## 2 Hybrid Threats

The NATO Glossary of Terms and Definitions, found in AAP-6, formally defines hybrid threats as “a type of threat that combines conventional, irregular and asymmetric activities in time and space.” [14] The NATO definition emphasizes the fusion and synergy aspects of the threat but uses broad categories for the types

of activities. The NATO Strategic Communications Centre of Excellence (StratCom COE) provides sample activities in stating the term hybrid describes “a wide array of measures, means and techniques including, but not limited to: disinformation; cyberattacks; facilitated migration; espionage; manipulation of international law; threats of force (by both irregular armed groups and conventional forces); political subversion; sabotage; terrorism; economic pressure and energy dependency.” [15] StratCom COE focuses on the characteristics of hybrid threats, with the most prominent being actions “coordinated and synchronized across a wide range of means.” These actions aim to “influence different forms of decision-making at the local (regional), state, or institutional level.” Those decisions can be made by political leaders, the general public, or military members, at the strategic or the tactical level of warfare. StratCom COE emphasizes that hybrid threats act as levers of influence using combinations of activities that span instruments of power, including Diplomatic, Information, Economic, and Military. StratCom COE admits that definitions of hybrid threats “lean heavily on Russian actions in Ukraine and Crimea.”

Associate Professor Bettina Renz remarks that “in the aftermath of the Crimea annexation in March 2014, the idea of hybrid warfare quickly gained prominence as a concept that could help to explain the success of Russian military operations in this conflict.” [16] She notes that Russia’s swift victory in Crimea stood in stark contrast to previous campaigns in Chechnya and Georgia, which were primarily fought by heavy-handed conventional forces. Instead, Russia used a combination of military and non-military means in a covert manner in Crimea and Eastern Ukraine. Senior Research Fellow Andras Racz outlines Russian hybrid operations in three main phases based on concrete events [17]. In the first, the preparatory phase, Russia creates the means to capitalize on weakness and vulnerabilities of the target country. Those means include by establishing loyal political and cultural organizations, bribing officials and officers, contacting local organized crime groups, building media positions, launching disinformation campaigns, and fostering anti-government sentiments. In the second, the attack phase, Russia launches organized, armed violence. In both Crimea and Eastern Ukraine, unmarked military personnel setting up checkpoints and overrunning government buildings, while demonstrators in civilian clothes took over media television and radio outlets. Meanwhile, massive regular military units were positioned on the border with Ukraine. In the third, the stabilization phase, illegal referendums take place. In both regions, those showed support for independence, which resulted in the annexation of Crimea and the establishment of Separatist republics.

Journalist Sam Jones at the Financial Times claims Russia had found a “new art of war” in their intervention in Ukraine [18]. Jones says the most lucid exposition of the new concept known as “hybrid war” is contained in an article by Valery Gerasimov, the Chief of the Russian General Staff, in a Russian defense journal in February 2013. In it, Gerasimov lays out his perspective on current and future warfare for a Russian audience. He highlights that war is now conducted by “a roughly 4:1 ratio of non-military and military measures.” [19] A graphic in the paper depicts the range of non-military measures to include diplomatic pressure, economic

sanctions, and political opposition, along with military measures to include strategic deployment, all underpinned by information conflict. Gerasimov also identifies new forms and methods for warfare to include the use of asymmetric and indirect operations. His views on warfare presented in the article became known in the West as the Gerasimov Doctrine, for the way Russia conducted operations in Ukraine a year later. Although in Russian intellectual circles, the idea of hybrid war is a completely Western concept, used to foment a “color revolution” for a forced change of political regime. The Gerasimov article cites examples of supposed Western efforts to change unfavorable leadership in Iraq, Syria, and Kosovo.

Researcher Ofer Fridman explains that Russian scholars and strategists interpret the Western theory for hybrid war in the context of Russian political–military experience, to conceptualize the Russian counterpart called *gibridnaya voyna*. This term is a direct translation of the Western term hybrid warfare. Yet, the Russian concept is broader in scope and involves “all spheres of public life: politics, economy, social development, culture.” ([20], 45) Fridman suggests the Russian view is based on the notion of subversion in war, expressed by philosopher Elliot Messner over 60 years ago. In subversion war, fighters are not just the troops, but also public movements. The most distinguishing characteristic of the subversion war is the psychological dimension of warfare. In the contemporary version of *gibridnaya voyna*, the aim is to first “break the spirit of the adversary’s nation by a gradual erosion of its culture, values, and self-esteem; and second, an emphasis on political, informational (propaganda) and economic instruments, rather than on physical military force.” ([20], 45) In *gibridnaya voyna*, these instruments, coupled with innovative military and information technologies, undermine the political legitimacy of an adversary.

Senior fellow Mark Galeotti states a range of deniable irregular actors, from volunteers and mercenaries to militias and gangsters, are used by Russia to generate military capabilities with political utility. He claims that Russia armed forces, in addition to their obvious value in full-scale conflict, are “useful for coercive diplomacy and heavy-handed messaging.” [21] Displays of Russian military force are used in brinkmanship and for intimidation. During the threat of invasion in 2022, Russia conducted military exercises with Belarus that involved 30,000 troops near Ukraine’s border. They were extended to supposedly “prevent provocative actions by the armed forces of Ukraine against our country and Belarus.” [22] The drills included test launches of Russian strategic missiles, overseen by President Putin and his Belarusian counterpart Alexander Lukashenko. A Kremlin press office release stated Russian aerospace forces launched Kinzhal hypersonic missiles, Northern and Black Sea Fleet ships and submarines launched Kalibr cruise missiles and Zirkon hypersonic missiles, and ground forces launched the Iskander land-based cruise missile from the Kapustin Yar test site [23]. The military activities served as a diplomatic instrument to impose Moscow’s will upon NATO to accept their security demands. The conduct of the drills and tests, along with the massing of troops and advanced weapons on the border, amplifies an assertion by Galeotti that the military has a distinct role “in pursuit of Moscow’s wider strategic goal

of dividing, distracting and demoralizing the West.” That role was amplified as the Russian invasion shifted into a classical way of brutal siege warfare.

### 3 Emerging Technologies

The 2018 US National Defense Strategy noted that the increasingly complex security environment is affected by “rapid technological advancements and the changing character of war.” [24] It asserts that competitors and adversaries will seek to optimize new technologies that are “moving at accelerating speed.” They will use these innovations in a more lethal and disruptive battlefield across domains, and in other areas of competition short of open warfare. Those areas encompass information warfare, denied proxy operations and subversion, hallmarks of hybrid war. New technologies include:

Advanced computing, big data analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology.

The 2018 US National Defense Strategy construes that nation state access to these emerging technologies will erode US conventional overmatch. Furthermore, the 2020 US National Strategy for Critical and Emerging Technologies details aspirations by China and Russia to obtain such technological advancements [25]. It emphasizes that China is “dedicating large amounts of resources in its pursuit to become the global leader” in both science and technology. Furthermore, China is “implementing a strategy to divert emerging technologies to military programs, referred to as military-civil fusion,” whereas Russia is focusing government-led efforts “on military and dual-use technologies, such as artificial intelligence, that it believes will bring both military and economic advantages.” However, like China, the strategy claims that Russian will also enable “its defense industrial base through civil-military integration.”

The 2020 US National Strategy for Critical and Emerging Technologies describes these sorts of technologies as “identified and assessed by the National Security Council (NSC) to be critical, or to potentially become critical, to the United States’ national security advantage, including military, intelligence, and economic advantage.” A 2022 report by the Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council provides the following updated list of technology areas deemed particularly important to US national security [26]:

- Advanced Computing • Advanced Engineering Materials • Advanced Gas Turbine Engine Technologies • Advanced Manufacturing • Advanced and Networked Sensing and Signature Management • Advanced Nuclear Energy Technologies • Artificial Intelligence • Autonomous Systems and Robotics • Biotechnologies • Communication and Networking Technologies • Directed Energy • Financial Technologies • Human-Machine Interfaces • Hypersonics • Networked Sensors and Sensing • Quantum Information Technologies • Renewable Energy Generation and Storage • Semiconductors and Microelectronics • Space Technologies and Systems

The Fast Track Action Subcommittee report also contains key subfields that describe the scope of each technology area in more detail.

NATO recognizes that emerging technologies “are changing the nature of peace, crisis, and conflict.” It is adopting an implementation strategy for seven key disruptive technologies [27]:

Artificial intelligence, data and computing, autonomy, quantum-enabled technologies, biotechnology, hypersonic technology and space.

NATO plans to develop individual strategies for each, with the priority being artificial intelligence and data [28].

This chapter selects three emerging technologies to explore that are common in the US and NATO lists: artificial intelligence, autonomy, and hypersonics. The three are being advanced and exploited by China and Russia in novel forms of warfare although the focus here will be on Russia as a hybrid threat empowered by the three technologies.

### ***3.1 Artificial Intelligence***

In September 2017, President Putin declared that the nation that leads in Artificial Intelligence (AI) “will become the ruler of the world.” [29] He further illuminated that AI “comes with colossal opportunities, but also threats that are difficult to predict.” This determination is because AI promises to boost countries’ economies but will also be useful in warfare. IBM states that artificial intelligence “leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind.” [30] IBM explains that AI “combines computer science and robust datasets, to enable problem-solving.” The field also encompasses machine learning and deep learning. IBM construes that AI algorithms are used to create “expert systems which make predictions or classifications based on input data.” AI is classified as either narrow, where systems are trained to perform specific tasks, or strong, where machines have self-awareness equaled to humans. A Congressional Research Service (CRS) Report expounds that narrow AI is integrated into a variety of military applications, such as intelligence, surveillance and reconnaissance, logistics, cyberoperations; command and control; and semi-autonomous and autonomous vehicles. Narrow AI technologies are intended to augment or replace human operators. The CRS Report highlights that AI-enabled systems can “react significantly faster than systems that rely on operator input” and “cope with an exponential increase in the amount of data available for analysis.” [31]

AI technology can accelerate part of the list of StratCom COE hybrid threat measures, means, and techniques, particularly disinformation, that seeks to influence decision-making by leaders and the populace. CRS Researcher Kelly M. Saylor finds that AI can enable “increasingly realistic photo, audio, and video digital forgeries, popularly known as ‘deep fakes’.” [31] She notes that deep fake

technology could “generate false news reports, influence public discourse, erode public trust, and attempt blackmail of government officials.” Russia exploited deep fake technology to target and amplify public debate during the 2020 US Presidential Election. Russian internet trolls formally associated with the notorious Russian Internet Research Agency created and ran a news website called Peace Data. They hired unaware real-life journalist to write articles on topics such as corruption, abuse of power, and human rights violations, with the aim to divide Democratic voters. While the freelancers were real reporters, editors for the site “were personas whose profile pictures were deepfakes, or algorithmically generated.” ([32], 3) The mixture of real persons writing the content and presumably amplifying it, made it difficult for social media tech companies to identify the activity as a subtle influence operation and block it.

Deep fake technology also appeared during the Ukraine war in an attempt to influence Ukrainian fighters. In a deep fake video, Ukrainian President Zelensky is supposedly surrendering to Russia. He appears to stand behind a white presidential podium and backdrop that both display the country’s coat of arms. Zelensky slowly and deliberately speaks in Ukrainian, saying “I ask you to lay down your weapons and go back to your families.” [33] However, Professor Hany Farid said there are several obvious signs the video is a deep fake. It is low-quality and low-resolution, without much motion [34]. Even still, the widely spread deep fake video cast doubt during a tense time for the population. Another part of the StratCom COE hybrid threat menu that is prime for AI technology acceleration is cyberattacks. Researchers Nektaria Kaloudi and Jingyue Li outline the “application of AI-driven techniques in the attack process, which can be used in conjunction with conventional attack techniques to cause greater damage.” [35] They present case studies for how AI can be a basis to launch cyberattacks. For example, in a new class of evasive next-generation malware that uses deep learning algorithms to perform malicious tasks, or in password brute-force attacks using an intelligent dictionary based on patterns derived from prior password, or by intelligent social bots that spread machine-generated content automatically without a command-and-control channel. The authors map the AI-based cyberthreats across the Cyber Kill Chain to illustrate impact while AI advantages to target, aid, conceal, automate, and evolve are clear, in reality, the destructive wiper attacks seen in Ukraine in 2022 leading up to the invasion appear to still use conventional attack techniques [36].

The aforementioned CRS Report also contends that AI-enabled systems could “enable new concepts of operations such as swarming (i.e., a cooperative behavior in which unmanned vehicles autonomously coordinate to achieve a task) that could confer a warfighting advantage by overwhelming adversary defensive systems.” [31] Russian forces tested a form of “swarm” drones in combat in Syria in 2019 and 2020 before invading Ukraine. They employed the KYB Kub (Cube) and its successor, the Lancet-3 which are small kamikaze drones, often called loitering munitions. Both are built by ZALA, the Kalashnikov Design Bureau (part of Rostec). The twenty-six-pound Lancet-3, reportedly executed “dozens of precision strikes” with “high efficiency.” [37] Videos released by Russian media show the Lancet-3 diving toward the truck of a local commander and also striking a machinegun position. The Lancet-

3 is launched from a simple catapult but there is no recovery provision. It flies at fifty-to-sixty miles per hours for about 40 min. It can be given coordinates to attack, or an operator can search for targets. Upon acquisition, the drone plunges down, with operator course corrections, to detonate a 6.6-pound warhead. The earlier version, the Kub, did not have the video feed adjustment capability. ZALA is also working on a different operational concept for the Lancet, to use it in an “aerial minefield” to intercept enemy drones. A swarm of Lancets would orbit overhead friendly troops in a 20-mile-square-box and ram any incoming hostile drones [38].

### 3.2 *Autonomy*

The two operational concepts described for the Lancet drone represent semi-autonomous (operator adjusts trajectory) and autonomous (itself rams enemy drones) AI-driven applications. A US Department of Defense Directive defines autonomous weapon systems as a class “capable of both independently identifying a target and employing an onboard weapon to engage and destroy the target without manual human control.” [39] That contrasts with the Directive definition of semi-autonomous, where weapons systems “only engage individual targets or specific target groups that have been selected by a human operator.” The Russian military employed semi-autonomous drones extensively in Eastern Ukraine before their invasion. The Russians would identify a target with a high-level drone and pass the sighting off to another lower-level drone that would fix the target coordinates. Then, the Russians would adjust their artillery firing solutions with the drone. This target acquisition and destroy cycle can be done in as little as 10–15 min [40]. The drones can also collect signals intelligence or act as an airborne electronic warfare jamming platform. The drones used in the Donbass include the Forpost with a maximum altitude of 6300 m, Orlan-10 at 5000 m, and the Dozor-100 at 4200 m. Payload options can include infrared video, daylight video, laser range finder, and still camera.

Russia is developing an AI-enabled rotary-wing type drone named Termit. The reconnaissance and strike helicopter drone have autonomous features. Termit will be equipped with ISR sensors and carry 80 mm laser-guided missiles and unguided munitions. Initially, an operator will identify and designate a target. Then, the drone can “act autonomously with the help of artificial intelligence algorithms embedded in the drone control system that allow Termit to choose the most optimal route to target.” Finally, upon target acquisition, the decision to launch a weapon is made by the operator [41]. Another Russian drone under design named Grom will be capable of control by human operators but also acting fully autonomously. Operators will give voice commands to Grom but it “will perform those tasks completely autonomously.” [41] A third Russian drone under development, the Okhotnik, will be able to operate without communicating with a human operator. While flying as a wingman to manned Su-57 fighters, the drone will be capable of returning to base if it loses connection and communication with the pilot. An AI-enabled operating



system will eventually allow the Okhotnik to “perform combat missions in a fully autonomous mode.” [41]

Russia has also tested its Orion unmanned air vehicle in a “drone killer” mode against a rotary-wing drone. The Ministry of Defense released a video showing Orion “firing a new version of the 9M113 Kornet anti-tank guided missile (ATGM) against the helicopter drone.” ([42], 26) The engagement began at 60 miles apart and the firing occurred at 2.5 miles. The head of the Russian General Staff Office for drone development claims the Orion can shoot down the Turkish-made Bayraktar TB2 drone. A statement intended to be a clear signal to Ukraine who acquired the TB2. Russia has also progressed in the development and fielding of ground robots. For the first time, two remote-controlled unmanned ground vehicles were deployed in combat formations during the Zapad military exercise with Belarus in September 2021. The Russian Ministry of Defense reported that the Uran-9 engaged targets at more than 3 miles. Uran-9 is a tracked vehicle “equipped with a 30mm autocannon, anti-tank missiles and a flamethrower.” ([43], 4, 6) Russia previously tried to use a Uran-9 prototype in Syria. The second vehicle was the smaller Nerekhta that carries a mounted machine gun and a grenade launcher. The breakthrough use of the robots highlights the potential to move to more AI-enabled autonomous operations.

The US Army Asymmetric Warfare Group proclaims that Russia’s use of drones proved “to be a game changer in Eastern Ukraine.” [40] Their dubious use by proxy forces in a frozen conflict at the time is a hallmark of a hybrid threat. The drones enabled the separatists to achieve fire superiority over a heavy conventional force in decentralized operations. Russia was able to deny involvement while achieving political objectives. Experts believed that Russian fleets of “killer robots” were likely to be a potent weapon in the invasion of Ukraine [44] although reporting is limited on their employment by the Russian invaders. Early in the war, the Russian Ministry of Defense released a video of the Orion drone striking a ground target in the Donetsk region while wreckage of other Russian drones, including the Forpost-R, Orlan-10, and even the Kub loitering munition, indicate a variety have been used to some extent [45]. Senior Research Fellow Brendan Walker-Munro offers potential reasons for less than widespread usage. They could be held in reserve or hampered by logistic breakdowns [44]. Even still, evidence for the use of drones with some autonomous capabilities demonstrates that Ukraine is a proving ground for AI-enabled technologies.

Subsequent large-scale fielding of AI-enabled autonomous systems is important to Russia to achieve military objectives. Autonomy enables reach and persistence deep into contested zones and independent operations in denied communications environment. AI-enabled autonomous systems are durable and expendable. They can conduct dangerous missions to reduce risk to human lives, especially before permissive conditions are established. For example, the Nerekhta unmanned ground vehicle delivered ammunition and equipment during the Zapad exercise, in addition to conducting fire support ([43], 4, 6). Autonomy also speeds the decision cycle by automated target acquisition and engagement without a human in the loop. While AI-enabled autonomous weapons provide tactical advantage in target processing, they create considerable ethical concerns in target selection and kill decisions.



The main concern being the machines will unwittingly kill innocent civilian non-combatants. Distinguished Professor Emeritus John Arquilla notes that heated discourse on so-called killer robots occurring in democracies is slowing their development although he is quick to point out that “neither China nor Russia has shown even the very slightest hesitation about developing military robots.” [46]

### 3.3 Hypersonics

On March 1, 2018, President Putin gave his *poslanie*, or State of the Nation speech to the Russian Federal Assembly. The location was moved from normal Georgievskii hall in the Kremlin to the Manezh to accommodate picture displays and video clips. The first part of the speech for 70 min concentrated on domestic matters, which received polite applause, while the second part for 45 min that addressed international relations and defense garnered standing ovations. Putin outlined the need to counter attempts by the United States to weaken Russian strategic deterrence which equated to an obligation to develop an array of new weapons to overcome the US missile defense network [47]. Putin spoke in front of large screens displaying vivid images of the weapons. An animated video showed “a cruise missile fired from northern Russia flying across the Atlantic Ocean, evading missile defenses, then circling around the southern tip of South America before heading north toward the U.S.” [48] While boasting about Russian military prowess, Putin focused in the elaborate video on a design vulnerability for American defenses. They are based on high-flying ballistic missiles that can be destroyed in the atmosphere. Instead, Putin said the new class of Russian weapons “travel low, stealthily, far and fast – too fast for defenders to react.” [49] For which, Putin labeled the weapons as “invincible.”

Putin described a total of six weapons systems. In order, the Sarmat, a heavy Intercontinental Ballistic Missile; the Burevestnik, the nuclear-powered cruise missile in the video; the Poseidon, an armed nuclear-powered underwater drone; the Kinzhal, a hypersonic missile launched from a supersonic aircraft; the Avangard, a hypersonic glide vehicle for an Intercontinental Ballistic Missile; and the Peresver, a combat laser weapon [47]. A third hypersonic weapon, the Tsirkon, fired from surface ships, has also been in development. Hypersonic weapons fly at speeds of Mach 5 (five times the speed of sound) or more [50]. They do not follow a set trajectory but instead maneuver at low altitude on route to their target. The two primary categories of hypersonic weapons are hypersonic glide vehicles released from rockets to glide to a target or hypersonic cruise missiles that are powered by air-breathing engines. Russian hypersonic weapons are potentially armed with nuclear warheads whereas conventionally armed hypersonic weapons rely on kinetic energy to impact and destroy targets, which means greater accuracy is required to be effective. The unique features of the weapon in speed, maneuverability, and altitude are aptly suited to penetrate existing missile defenses and destroy their high-value targets.

In October 2018, President Putin bragged at an international policy forum in Sochi, Russia that new hypersonic missiles give his country a military edge. Putin said “We have run ahead of the competition. No one has precision hypersonic weapons.” [51] He reiterated that stance in December 2019 at a meeting with his top military officers. Putin told them “Now we have a situation that is unique in modern history when they [the US] are trying to catch up to us.” [52] Putin referred to the pending deployment of the Avangard and the Kinzhal already in service. The Avangard hypersonic glide vehicle became operational a few days later [53]. It entered combat duty with a missile unit in the Orenburg region in the southern Urals Mountains. Avangard had passed its test program a year earlier with a flight of 6000 km, where it maneuvered “horizontally and vertically at hypersonic speeds” before engaging a simulated target at the Kara range in Russia’s Kamchatka peninsula. The hypersonic glide unit supposedly flies at Mach 27. It has been integrated with the Soviet built RS-18B Intercontinental Ballistic Missile, which will carry six of the hypersonic glide vehicles. The launch of multiple independently targeted re-entry vehicles (MIRV) will further complicate the tracking solutions of missile defenses.

The Kinzhal hypersonic missile first debuted at the Victory Day military parade in May 2018, only months after Putin’s speech on the new super weapons ([54], 1–2). It was carried underneath a Russian MIG-31K fighter in flight. The Kinzhal was successfully tested in July 2018, in a launch from a MIG-31K, NATO code name Foxhound, that struck a target 500 miles away. Russia claims Kinzhal can reach Mach 10, when fired from the MIG-31 [50]. Kinzhal is suspected to be a modified Iskander conventional missile, which reaches its Mach speeds only when fired from a high-speed, high-altitude launch vehicle [47]. Russia deployed MIG-31 warplanes armed with Kinzhal for the first time outside its borders to Syria in June 2021 [55]. The Tsirkon (or Zircon) is a ship or submarine launched missile capable of reaching speeds of Mach 6 to Mach 8 [50]. It can supposedly strike both ground and naval targets at a range of 250–600 miles. Evidence of these claims emerged in July 2021 when the Admiral Gorshkov frigate fired a Tsirkon missile in Russia’s Arctic region. It flew at Mach 7 to hit a surface target at 217 miles [56]. In October, the Severodvinsk nuclear submarine fired a Tsirkon missile that hit a target in the Barents Sea ([57], 1). Further Tsirkon tests occurred in December 2021, with 10 fired from a frigate and two more from a submarine. Putin lauded the weapon as “part of a new generation of unrivalled arms systems.” ([58], 2–4, 14–15)

Russia launched hypersonic missiles for the first time in combat during its invasion of Ukraine. On March 18, 2022, Kinzhal missiles destroyed a large Ukrainian warehouse of missiles and ammunition in the village of Delyatin. The next day, Kinzhal missiles hit a Ukrainian fuel depot in Kostiantynivka near a Black Sea port, as part of a coordinated strike with Russian warships firing cruise missile from the Caspian Sea. President Biden said “It’s a consequential weapon . . . It’s almost impossible to stop it. There’s a reason they’re using it.” [59] While the hypersonic missile firings were against large stationary targets, they were likely tests of the weapon and intended to send a message to the West. That message, at least for now, is that Russia has the edge in hypersonic technology.

Russia intends to use hypersonic technology to change the mutual nuclear deterrence paradigm, by altering the balance of strategic stability. Russia views strategic stability as primarily nuclear parity with the United States. Implementation of strategic stability is ensured by an appropriate relationship between strategic offenses and defenses. Putin's apparent reason to create so-called invincible weapons was based on his perception that the US missile defense network negatively affected strategic stability. The perception became acute when the US decided to place missile interceptors in Europe, supposedly to protect against ballistic threats from North Korea and Iran but suspected to be directed toward Russia. Thus, hypersonic technology is important to Russia to meet national interests. If the speed, stealth, and altitude of hypersonic weapons can defeat the US missile defense network, then the strategic balance tilts back into Russia's favor. Russian military and political leaders believe "there is no alternative to mutual nuclear deterrence." [60] After an April 2022 test of the heavy Intercontinental Ballistic Missile Sarmat, expected to carry the nuclear armed Avangard hypersonic glide vehicle, all the way to the continental United States, President Putin congratulated the military, saying the successful launch would "give thought to those who are trying to threaten Russia." [61]

## 4 Resilience Approach

Resilience means "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." [62] In regard to hybrid threats, that means to withstand attacks that penetrate defenses, by speed, stealth, or maneuver, or withstand attacks that overwhelm defenses, by resource concentration, mass, or volume. NATO finds in the 2021 Communique that "resilience is essential for credible deterrence and defense." While NATO recognizes that resilience is "a national responsibility," it is committed to working "closely with our partners . . . to make . . . our broader neighborhood more secure." One of those partners is Ukraine, for which NATO decrees they "stand firm in our support for Ukraine's right to decide its own future and foreign policy course free from outside interference." That firm support became evident in financial aid and weapon shipments to Ukraine for deterrence and defense against Russian invaders. The United States alone pledged over \$1 Billion in military aid to Ukraine, and at least 30 other countries provided military assistance, including \$551 Million from the European Union [63]. US shipments are a mixture of weapon systems, like Javelins and Stingers, and support and sustainment items, to include "food, body armor, helmets small arms and ammunition, medical and first aid kits." [64] After a call for help from Ukraine to build cyber resilience, the European Union deployed a Lithuania-led cyber rapid-response team, with cyber experts from Croatia, Poland, Estonia, Romania, and the Netherlands remotely and on site in the country [65].

Resilience usually occurs when a traumatic event, such as disaster, terrorism, or war, shocks and disrupts a system. Scholars Tomas Jermalavicius and Merle Parmak find that resilience is “more than the ability to endure pain, it is the ability to find unknown inner strengths and resources, to cope effectively with long-term pressures.” [66] They point out that resistance is another type of stressor coping mechanism. Jermalavicius and Parmak define resistance as the “mobilization and deployment of a system’s resources to cope with the immediate effects of stressors.” The United Kingdom Ministry of Defense determined that Russia has been “surprised by the scale and ferocity” of Ukrainian resistance, which stems from adaption and flexibility inherent in resilience [67]. In the first 2 days after the Russian invasion began, 40,000 ordinary citizens found inner strength to join the Territorial Defense Forces [68]. They constructed and man military defenses consisting of metal anti-tank barriers, concrete blocks, and sandbags. Those that were turned away still help by making Molotov cocktails, sewing camouflage nets, or distributing food to the volunteer soldiers. Likewise for cyberspace, Ukraine created a special IT army, comprised of volunteer hackers and IT specialists from around the world. An official at the Ukrainian cybersecurity agency said the goal of the IT army is to “do everything possible . . . to make [the] aggressor feel uncomfortable with their actions in cyberspace and in Ukrainian land.” [69] The IT army launched attacks against Russian and Belarusian websites and data exposure operations against their officials. They succeeded in taking down sites for the Kremlin, Russian state-owned Sberbank, Radio Belarus, and others [70].

Stout Ukrainian resistance on the ground and in the air against the Russian military onslaught has been partly enabled by Western-supplied shoulder-fired missiles, in particular the FGM-148 Javelin anti-tank weapon and the portable FIM-92 Stinger anti-aircraft missile. Turkish-made Bayraktar TB2 armed drones have also offset Russia’s enormous military advantage. The TB2 can take off, land, and cruise autonomously, with a human operator decision to launch laser-guided bombs. The array of compact high-tech weapons has exacted a high toll on Russian forces. The Ukraine government claims to have destroyed more than 400 Russian tanks along with many other less-armored vehicles [71]. Ukraine flipped the Russian script on the use of armed drones to attack separatists in the Donetsk region in October 2021. When pro-Russian forces opened fire on Ukrainian positions with a D-30 howitzer, a Ukrainian controlled TB2 drone flying in the vicinity struck the cannon with a missile [72]. Days after Russian forces entered Ukraine, another TB2 destroyed a Russian mobile-air-defense system along a road with a missile [73]. Russian use of highways for convoys has enabled further TB2 drone strikes. Ukrainian operators also attack at night with modified octocopter drones when Russian forces are static. Heavy duty R18 model octocopter drones with thermal cameras have dropped 5 kg anti-tank grenades to destroy tanks and electronic warfare trucks [74].

Ukrainian President Zelensky pleaded directly to members of both chambers of Congress in a virtual address for the United States to help create a no-fly zone over Ukraine [75]. He also asked for the United States to provide air defense systems, such as the Russian-made S-300 surface-to-air missile system. The Stinger

is only effective against helicopters and low-flying aircraft. While the no-fly zone would potentially stop Russia bombers from harming civilians, the S-300 system would theoretically defeat the barrage of conventional missiles. The United States decided to send some of its secretly acquired Soviet-style air defense weapons, including the SA-8 but not the S-300. The United States hoped the equipment “will enable Ukraine to create a de facto no-fly zone.” [76] Although none of these systems would be able to sufficiently counter the Russian hypersonic missile threat, hypersonic weapons “challenge detection and defense due to their speed, maneuverability and low altitude of flight.” [50] These characteristics mean detection by ground-based radars is very late in flight, which limits the ability of defensive systems to intercept the weapon. The late detection also hampers the ability of command-and-control systems to process data and react fast enough to fire interceptors. While point defense systems could attempt to deal with the threat, they can only defend small areas, not the range of targets seen in the Ukraine war.

## 5 Future Applications

Russia attempted to employ hybrid threat tactics to coerce NATO into accepting untenable security demands. When negotiations stalled, Putin elected to proceed with the military instrument to achieve his goals by force. The West responded with severe sanctions on Russian oligarchs, industries, and banks, while countless American companies severed operations in Russia. The effect will contract the Russian economy by 10% for a year and stagnation will hamper military production for years to come [77]. Meanwhile, Ukraine soldiers and volunteers displayed ferocious military resistance, through heroic strength found in national resilience. Their use of Western-supplied asymmetric anti-tank weapons in ambushes and skirmishes decimated Russia’s larger and heavily armed military [78]. At the time of this writing, the Pentagon estimates Russia “has between 85 and 90 percent of its ‘combat power’ remaining” from the invasion force of about 150,000 personnel [79]. To shore up unexpected combat losses, Russia resorted to bringing in reinforcements from the separatist republics of South Ossetia and Abkhazia in Georgia. In whatever fashion this terrible war plays out, the outcome will be a depleted Russian ground force with low stocks of missiles and rockets. That doesn’t mean the Russian military will not be a menace to the West, as other combat elements, like sophisticated nuclear submarines, advanced naval combatants, long-range bombers, autonomous air and ground robots, and hypersonic weapons, that can be fired from land, air, or sea, will still exist.

While an arsenal of hypersonic missiles will empower Russian with an invincible means of strategic deterrence, any future employment of conventional forces in the territory of NATO nations would bring the rath of their collective military might under Article 5 for self-defense. Instead, Russia will mostly likely revert to being a hybrid threat that capitalizes on non-military instruments in the prescribed 4:1 ratio. They can use covert means for direct action by special forces or military intelligence

agents. Even turn to mercenaries in private military contractor groups for deniable operations. For example, United Kingdom officials claimed the Russian mercenary company Wagner Group has been tasked to kill Ukrainian President Zelensky [80]. Russia can also conduct shady disinformation campaigns to influence sympathetic and unaware audiences. For example, during the Ukraine war, groups linked to Russia and Belarus posed as independent news outlets and journalist online to push Russian talking points [81]. Those points can be enhanced with AI-enabled deep fakes in the form of realistic photo, audio, and video digital forgeries. Russia can also move beyond the traditional playbook of hacks and botnets, to AI-enabled cyberoperations that overwhelm defenses [82]. The West has to be ready with resilience measures to withstand an array of hybrid threat activities empowered by emerging technologies.

## References

1. Krebs, K., Kwon, J.: Cyberattacks hits Ukraine Government Websites, CNN World, January 14, 2022
2. Microsoft Security: Destructive Malware Targeting Ukrainian Organizations, Blog Post, January 15, 2022
3. Karmanau, Y.: Ukraine claims Russia Behind Cyberattack in ‘Hybrid War’,” ABC News, January 16, 2022
4. Mecklin, J.: Introduction: the evolving threat of hybrid war. *Bull. At. Sci.* **73**(5), 298 (2017)
5. Marson, J., Volz, D.: Ukraine Government Websites Hit by Cyberattack, *The Wall Street Journal*, January 14, 2022
6. Polityuk, P.: Massive Cyberattack Hits Ukrainian Government Websites as West Warns on Russian Conflict, Reuters, January 14, 2022
7. Lubold, G., et al.: U.S. Officials Warn of Imminent Russian Invasion of Ukraine with Tanks, Jet Fighters, Cyberattacks, *The Wall Street Journal*, February 18, 2022
8. Antonov, D., Balmforth, T.: Russia Keeps Door Open After U.S. Rejects Key Security Demands, Reuters, January 27, 2022
9. Liptak, K.: Nord Stream 2 Pipeline Proves to be a Sticking Point in Biden and New German Chancellor’s Show of Unity, CNN Politics, February 7, 2022
10. Jordans, F.: German Caution on Arms to Ukraine Rooted in History, Energy, ABC News, January 25, 2022
11. Simmons, A.M.: Russia Confronts Ukraine with Upgraded Military Rebuilt After Soviet Collapse, *The Wall Street Journal*, February 1, 2022
12. Osborn, A., Nikolskaya, P.: Russia’s Putin Authorizes ‘Special Military Operation’ Against Ukraine.” Reuters, February 24, 2022
13. NATO: Brussels Summit Communique, Press Release (2021) 086, Issued 14 June 2021: para 3
14. NATO Standardization Office (NSO), AAP-6, NATO Glossary of Terms and Definitions, 2018
15. NATO Strategic Communications Centre of Excellence: Hybrid Threats: A Strategic Communication Perspective, Research Report, 2019: 8
16. Renz, B.: Russia and ‘hybrid warfare’. In: *Contemporary Politics*, vol. 22, no. 3, p. 283. Routledge (2016)
17. Racz, A.: Hybrid War in Ukraine: Breaking the Enemy’s Ability to Resist FIIA Report 43, pp. 57–66. The Finnish Institute of International Affairs (2017)
18. Jones, S.: Ukraine: Russia’s New Art of War, *Financial Times*, August 28, 2014

19. Bartles, C.K.: Getting Gerasimov Right, *Military Review*, January-February 2016: 34.
20. Fridman, O.: Hybrid warfare or Gibridnaya Voyna? Similar, but different. *Rusi J.* **162**(1), 43 (2017)
21. Galeotti, M.: *Russian Political War: Moving beyond the Hybrid*, p. 108. Routledge Press (2019)
22. Luxmoore, M, Forrest, B.: *Russia Extends Belarus Drills for Thousands of Troops as Ukraine Violence Escalates*, February 20, 2022
23. Dean, S., et al.: *Putin launches Russia's Ballistic and Cruise Missile Exercises*, CNN News, February 19, 2022
24. Secretary of Defense: *Summary of the National Defense Strategy of The United States of America*, 2018: 3
25. President of the United States, *National Strategy for Critical and Emerging Technologies*, October 2020: 1–2
26. National Science and Technology Council: *Critical and Emerging Technologies List Update*, February 2022: 2
27. North Atlantic Treaty Organization Public Diplomacy Division: *NATO 2030*, Fact Sheet, June 2021
28. Machi, V.: *Artificial Intelligence Leads NATO's New Strategy for Emerging and Disruptive Tech*, C4ISRNET, March 14, 2021
29. Vincent, J.: *Putin Says the Nations That Leads in AI 'Will be the Ruler of the World'*, *The Verge*, September 4, 2017
30. IBM Cloud Education: *What Is Artificial Intelligence (AI)*, IBM Cloud Learn Hub, June 3, 2020
31. Saylor, K.M.: *Emerging Military Technologies: Background and Issues for Congress*, CRS Report R46458, October 21, 2021: 2
32. Collier, K., Dilanian, K.: *Russian Internet Trolls Hired U.S. Journalists to Push Their News Website*, Facebook Says, NBC News, September 1, 2020
33. Metz, R.: *Deepfakes Are Now Trying to Change the Course of War*, CNN News, March 25, 2022
34. Metz, R.: *Facebook and YouTube Say They Removed Zelensky deepfakes*, CNN News, March 16, 2022
35. Kaloudi, N., Li, J.: *The AI-based cyber threat landscape: a survey*. *ACM Comput. Surv.* **53**(1), 21 (2020)
36. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation: *Destructive Malware Targeting Organizations in Ukraine*, Joint Cybersecurity Advisory, February 26, 2022
37. Roblin, S.: *Russian Drone Swarm Technology Promises Aerial Minefield Capabilities*, *The National Interest*, December 30, 2021
38. Hambling, D.: *Russia Plans 'Flying Minefield' To Counter Drone Attacks*, *Forbes*, April 20, 2021
39. Department of Defense Directive 3000.09: *Autonomy in Weapon Systems*, Updated May 8, 2017
40. Asymmetric Warfare Group: *Russian New Generation Warfare Handbook*, Version 1, December 2016: 23 (Unclassified Paragraph)
41. The Russia Studies Program: *AI and Autonomy in Russia*, Center for Naval Analysis, Issue 26, November 22, 2021: 3
42. Newdick, T.: *Russia's Predator-Like Drone is Now Shooting Down other Drones*, *The Drive*, December 20, 2021
43. Wellman, P.W.: *Zapad Military Drills Showcase Russian Unmanned Robots' Battlefield Breakthrough*, *Stars and Stripes*, September 15, 2021
44. Walker-Munro, B.: *Drones Over Ukraine: Fears of Russian 'Killer Robots' Have Failed to Materialize*, *The Conversation*, March 28, 2022
45. Atherton, K.D.: *How drones are Helping Fuel Propaganda in Ukraine*, *Popular Science*, March 28, 2022

46. Arquilla, J.: *Sitting Out of the Artificial Intelligence Arms Race Is Not an Option*, The National Interest, April 15, 2022
47. Cooper, J.: *Russia's Invincible Weapons: Today, Tomorrow, Sometime, Never?" Changing Character of War Centre*, University of Oxford, May 2018: 1
48. Grove, T., Gordon, M., Marson, J.: *Putin Boasts of New Nuclear Weapons*, The Wall Street Journal, March 2, 2018
49. MacFarquhar, N., Sanger, D.E.: *Putin's 'Invincible' Missile Is Aimed at U.S. Vulnerabilities*, The New York Times, March 1, 2018
50. Saylor, K.M.: *Hypersonic Weapons: Background and Issues for Congress*, CRS Report R45811, March 17, 2022: 1
51. Isachenkov, V.: *Putin: Russia 'Ahead of competition' with Latest Weapons*, Stars and Stripes, October 18, 2018
52. Associated Press: *Putin Says Russia is Leading World in Hypersonic Weapons*, Voice of America News, December 24, 2019
53. Associated Press: *Russia Commissions Intercontinental Hypersonic Weapon*, Voice of America News, December 27, 2019
54. Bodner, M.: *Russia's Hypersonic Missile Debuts Alongside New Military Tech at Parade*, Defense News, May 10, 2018
55. Isachenkov, V.: *Russia Launches Mediterranean Drills Amid Rift with Britain*, ABC News, June 25, 2021
56. Cole, B., *Russia Warns Pentagon That Hypersonic Missiles in Europe Could Lead to Conflict*, Newsweek, July 20, 2021
57. AFP: *Russia Test-Fires Hypersonic Missile from Submarine*, The Straits Times, October 4, 2021
58. Soldatkin, V.: *Russia Test-Fires New Hypersonic Tsirkon Missiles from Frigate, Submarine*, Reuters, December 31, 2021
59. Lendon, B.: *What to Know about Hypersonic Missiles Fired by Russia at Ukraine*, CNN World, March 22, 2022
60. Pavlov, A., Malygina, A.: *The Russian approach to strategic stability*. In: *The End of Strategic Stability?* p. 61. Georgetown University Press (2018)
61. Hodge, N., Pavlova, U.: *Russian Military Carries Out Test Launch of Sarmat Intercontinental Ballistic Missile*, Defense Ministry Says," CNN World, April 20, 2022
62. The White House: *Office of the Press Secretary, Critical Infrastructure Security and Resilience*, PPD-21 (February 12, 2013)
63. Debusmann, B. Jr.: *What Weapons Will US Give Ukraine – and How Much Will They Help?* BBC News, March 18, 2022
64. Kaufman, E.: *Pentagon: Half a Dozen "Shipments of Security Assistance to Ukraine from US aid Package" Already Arriving*, CNN News, March 31, 2022
65. Joe Tidy, "Ukraine: EU deploys cyber rapid-response team," BBC News, February 22, 2022
66. Jermalavicius, T., Parmak, M.: *Chapter 2: Societal resilience: a basis for whole-of-society approach to national security*. In: *Resistance Views*, pp. 26–27. Joint Special Operations University Press (2014)
67. Gigova, R.: *UK Defense Ministry: Russia has been "Surprised by the Scale and Ferocity" of Ukrainian resistance*, CNN Europe, March 19, 2022
68. Kottasova, I.: *Kyiv Has Transformed into a Fortress, with Its Residents Determined to Defend It*, CNN World, March 8, 2022
69. Lyngass, S., *Volunteer Hackers and IT Specialist Have Entered the Information War in Defense of Ukraine*, Official Says, CNN World, March 4, 2022
70. Toulas, B.: *Ukraine Says Its 'IT Army' has Taken Down Key Russian Sites*, Bleeping Computer, February 28, 2022
71. Wall, R., Michaels, D.: *Ukraine Has Become a Graveyard for Russian Tanks*, The Wall Street Journal, March 17, 2022
72. Forrest, B., Malsin, J.: *Ukraine's Use of Armed Drones Could Offset Some of Russia's Enormous Military Advantage*, The Wall Street Journal, February 20, 2022



73. Forest, B., Malsin, J.: Ukraine Leans on Armed Turkish Drones, Western Missiles to Thwart Russian Invasion, *The Wall Street Journal*, March 3, 2022
74. Parker, C.: An Elite Ukrainian Drone Unit Has Destroyed Dozens of ‘Priority Targets’ by Attacking Russian Forces as They Sleep, *The Times*, March 18, 2022
75. Quinn, M.: Zelensky Calls for No-Fly Zone over Ukraine in Emotional Plea to US Congress, *CBS News*, March 16, 2022
76. Youssef, N.A., Gordon, M.R.: U.S. Sending Soviet Air Defense Systems It Secretly Acquired to Ukraine, *The Wall Street Journal*, March 21, 2022
77. Hannon, P.: Sanctions sting Russian economy,” *Wall Street J.*, April 2–3, 2022
78. Marson, J., Michaels, D.: Ukraine’s Troops Fight War of Ambush and Skirmish Against Russian Invaders, *The Wall Street Journal*, March 21, 2022
79. Demirjian, K.: Russia Begins to Mobilize Military Reinforcements for Ukraine as Casualties Mount, Pentagon Says, *The Washington Post*, March 25, 2022
80. Colchester, M.: U.K. Says Russian Mercenary Group Aims to Assassinate Ukraine’s President, *The Wall Street Journal*, March 24, 2022
81. O’Sullivan, D., Lyngaas, S.: Ukrainian Soldiers’ Facebook Accounts Targeted by Hackers, Meta Says, *CNN World*, April 7, 2022
82. Warminsky, J.: US Says it Disrupted Russian Botnet ‘Before it Could be Weaponized’, *Cyber Scoop*, April 6, 2022

# Earthquakes—Management of Threats: A Holistic Approach



Eva Agapaki

## 1 Introduction

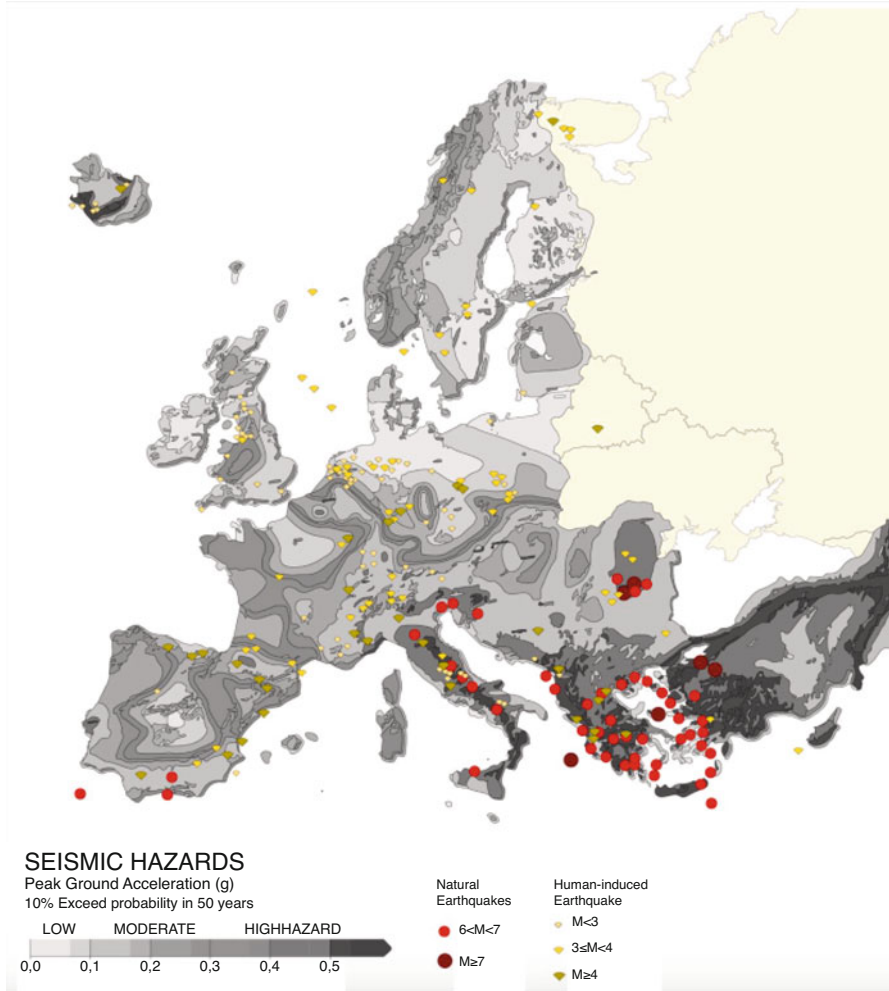
Earthquakes can cause irreversible damage to both the natural and built environments. They have incurred significant human casualties, with approximately 8.5 million people losing their lives and damages up to \$2 trillion since 1900 [22]. Earthquakes are one of the most devastating natural disasters, causing nearly 750,000 deaths globally, impacting more than 125 million people between 1998 and 2017, and causing \$ 661 billion in losses [84]. These impacts include human injuries, homelessness, displacements, or evacuations. Despite previous and ongoing research on earthquake hazard mitigation, uncertainty quantification of earthquake-induced damages, there are limited frameworks for stakeholders and policymakers to better assess seismic hazards and improve their decision-making processes.

Some recent major earthquakes have incurred substantial damages such as the 2012 Sumatra earthquake (8.6 magnitude), which caused 10 deaths and 12 injuries, and the 2011 Tohoku earthquake (9.1 magnitude), which destroyed over 100,000 buildings in Japan, caused nuclear disasters, and 10,000 deaths. The most powerful earthquake was recorded in Valdivia in 1960 with 9.5 magnitude. Earthquakes cause significant impacts on communities such as the collapse of buildings, water or power supply plants, and pose challenges in recovering and reconstructing structural systems. These challenges have raised the interest of multiple stakeholders, government agencies, and engineers.

Figure 1 shows a European map with the recorded geophysical events since 1970 related to a widely used parameter that describes the regions prone to seismic

---

E. Agapaki (✉)  
University of Florida, Gainesville, FL, USA  
e-mail: [agapakie@ufl.edu](mailto:agapakie@ufl.edu)



**Fig. 1** European map of the recorded seismic events since 1970 related to a seismic hazard map for the PGA with a 10% probability of exceedance in 50 years for stiff soil conditions. Map from the European Environment Agency (EEA) and the Human-Induced Earthquake Database

hazards, the peak ground acceleration (PGA). For each seismic zone in the figure, the PGA corresponds to the reference probability of exceedance in 50 years of seismic action for the no-collapse requirement. In Northern Europe, human-induced earthquakes (also known as HiQuakes) [82] are more frequent.

There are three main decision-making categories: (DC-a) *resource allocation* and (DC-b) *communication and planning*. DC-a decisions involve answering questions related to “How resistant should a structure be?” “What restrictions should be imposed for developments in high-hazard locations?” “How much should an

earthquake insurance policy cost?” DC-b decisions include scenarios that plan recovery and encourage citizen awareness, without necessarily necessitating the development of probabilistic models [42, 56, 79].

The structure of this chapter is as follows:

1. Introduction of seismic hazards and associated risks, analysis and hazard calculations, as well as basic earthquake management concepts
2. Overview of macroscopic earthquake management approaches (metrics and earthquake management tools) for the prediction of hazards and risks
3. Overview of microscopic earthquake management approaches (metrics and earthquake management tools)
4. Discussion and conclusions

## ***1.1 Definition of Earthquake Hazards and Risks***

Earthquake *hazards* are the natural phenomena resulting from earthquakes, while *risks* are the consequences of those hazards such as structural failures, fatalities, and economic losses. *Hazards* can be divided into two categories: *primary* and *secondary* hazards. Examples of primary hazards include ground shaking and permanent displacements (e.g., surface fault ruptures, uplift, subsidence, and folding). Secondary hazards are landslides, tsunamis, soil liquefaction, and floods. The focus of this chapter is centered toward management approaches for mitigating or predicting the consequences of primary hazards and risks. A comprehensive overview of probabilistic models used for hazard and risk analysis is given by [5].

## ***1.2 Hazard Analysis***

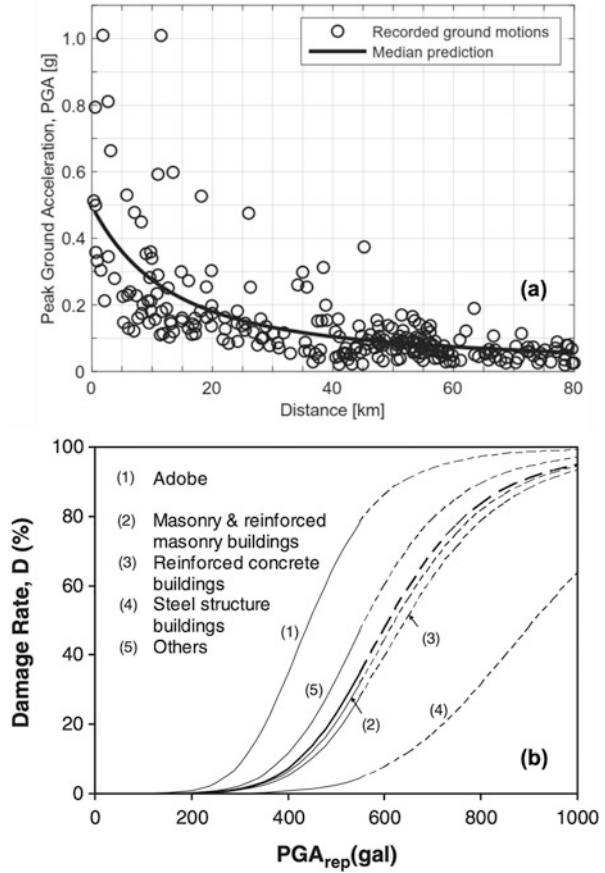
There are two widely adopted methodologies for identifying hazards and risks: deterministic and probabilistic. Many deterministic approaches have been proposed; however, there are three main limitations that question their use for hazard analysis:

1. The estimation of the magnitude of an earthquake that a fault (or a network of faults) produces is probabilistic. For example, the maximum magnitude ( $m_{max}$ ) can be computed either by statistical approaches using local data [40, 41]<sup>1</sup> or a Bayesian approach [20, 73] for regions of low seismicity where historical earthquake databases are too sparse.

---

<sup>1</sup>  $m_{max}$  is estimated by adding the largest observed earthquake magnitude in the region with the probability that  $x$  independent events should have magnitudes below  $m$ , assuming a magnitude-frequency distribution is considered. More information can be found at [5].

**Fig. 2** (a) Observed peak ground acceleration values from the 1999 Chi-Chi, Taiwan, earthquake and median predicted PGAs based on the Chiou and Youngs (2014) model [5] and (b) building fragility curves for various building types in the study area [67]



2. The distance of the earthquake rupture to the site of interest is not linearly correlated to the ground-motion intensity measures. For instance, we can consider a location close to two earthquake ruptures with the first source (S1) producing an earthquake of magnitude 5 at 0 distance from the source, and the second source (S2) producing an earthquake of magnitude 7 at a distance of 15 km. When using the predictive model of [16] to estimate the peak ground acceleration (PGA) and peak ground velocity (PGV) from each rupture, these are  $PGA_{S1} = 0.27g$ ,  $PGA_{S2} = 0.19g$  and  $PGV_{S1} = 13cm/s$ ,  $PGV_{S2} = 15cm/s$ . Therefore, the “worst case” rupture cannot be determined since the earthquake hazard is dependent on the choice of the ground-motion intensity metric. The variability of the ground motion intensity (PGA in Fig. 2a) illustrates that there is no clear upper boundary on the worst-case amplitude of the ground motion.
3. There is variability in impacts such as the structural damage, recovery costs, and time. The likelihood of these impacts needs to be quantified, so that decisions are

not conservative or progressive. Figure 2b illustrates fragility curves for different building types based on the 1999 Chi-Chi, Taiwan, earthquake.

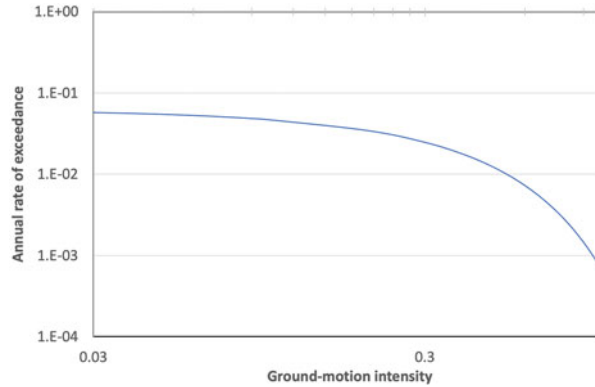
**Probabilistic Seismic Hazard Analysis** Therefore, the use of probabilistic models that determine the annual rate or probability of exceeding a specific level of shaking at a site of interest is recommended. The approach used to perform this analysis is called *probabilistic seismic hazard analysis* or PSHA. PSHA is the process by which ground-motion intensity measures are estimated for a site. PSHA requires seismic source characterization and the definition of ground motion prediction equations (GMPEs).

GMPEs are empirical and applicable to specific geologic/tectonic environments. The observations recorded during an earthquake event (i.e., ground-motion measurements and macroseismic intensities when available) are collected, sometimes corrected from the site amplification factors (in order to revert the measurements from soil conditions to rock conditions). These are then used to update the distribution of the ground-motion field, which is referred to as a shake-map. In other words, a shake-map is an estimate of the ground motion usually in the form of intensity measures (IMs) such as peak ground acceleration (PGA), spectral acceleration (SA), peak ground velocity (PGV), or macroseismic intensity. The main algorithms used to generate shake-maps are the USGS ShakeMap algorithms [77, 83] and the Bayesian inference method [30]. A comprehensive review of shake-map systems is provided by [33].

### 1.3 Ground-Motion Hazard Curves

Hazard curves are constructed by combining many models and data sources to quantify the probability of observing a specified PGA value or greater given an earthquake. An example hazard curve is illustrated in Fig. 3. This hazard curve could be computed by direct observations, simply by computing the fraction of years in which the PGA amplitude of interest is exceeded. However, this approach requires a large data set of PGA observations for the specific site. If a ground-motion intensity measure, such as PGA, has a probability of exceedance,  $p$ , in a year, we need at least  $1/p$  years to expect this PGA will be exceeded. In other words, we need at least  $1/p$  years of PGA data to estimate  $p$  from observations based on the Bernoulli trials principle. However, since many locations have not experienced strong ground shaking in the past decades, it is not feasible to forecast rare ground-motion shaking from just a few observations. Another limitation is the lack of ground-motion recording instruments (e.g., accelerometers) that are not available in many regions worldwide or even when available, they have recordings for a short observational period. Therefore, the use of direct observations to construct hazard curves cannot be widely applied.

**Fig. 3** Ground-motion hazard curve



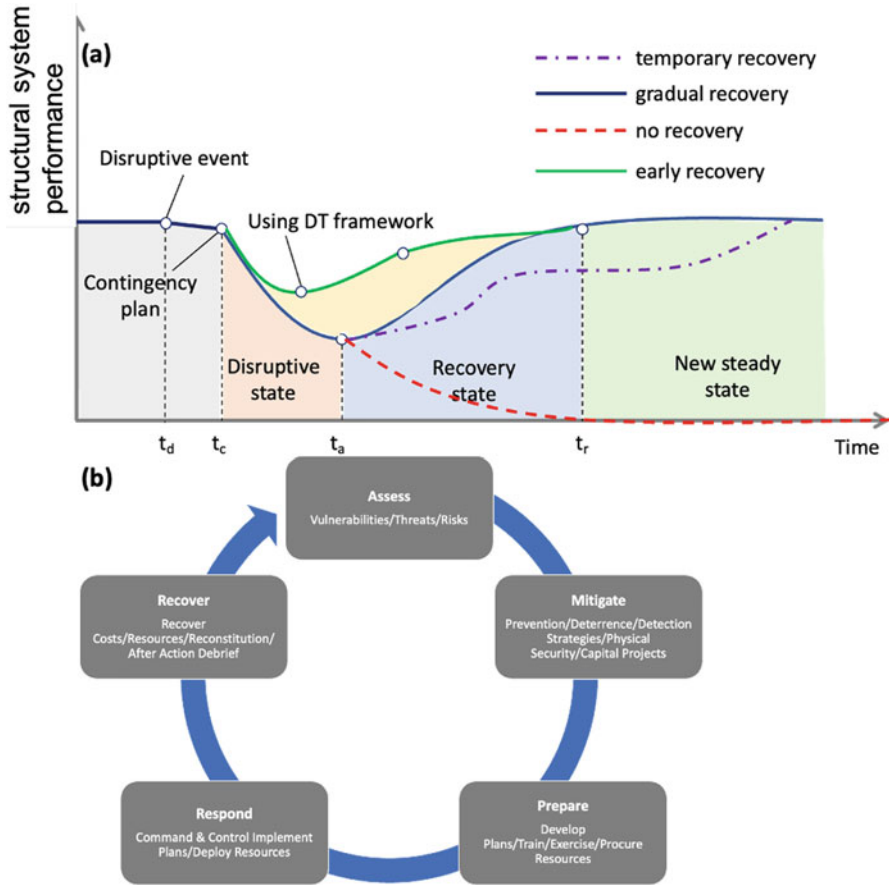
### 1.4 Seismic Resilience Concepts

Resilience incorporates the ability to (a) anticipate, prepare for, and adapt to changing conditions, (b) absorb, (c) withstand, respond to, and (d) recover rapidly from disruptive events. Those events can be either severe weather hazards (e.g., dense fog, flooding, snow, drought, tornado, wildfire, hurricane), threats (e.g., equipment outages, political changes, economic downturn, pandemics, cyberattacks, physical attacks), and vulnerabilities (e.g., equipment outages, lack of staff).

Resilience can be quantified by analyzing risks to a community (macroscopic level) or a building/building component (microscopic level). We adopt the definition of risks by the National Infrastructure Protection Plan (NIPP), where risk is defined by the likelihood and the associated consequences of an unexpected event [72]. Those risks are the hazards most likely to occur, potential threats, and vulnerabilities. Hazards and threats refer to incidents that can damage, destroy, or disrupt a site or asset. The difference between hazards and threats is that the former can happen unexpectedly, typically outside of a community's control, whereas the latter happen purposefully and are usually manmade. Some examples of hazards are natural hazards (e.g., hurricanes, earthquakes, wildfire), technological (e.g., infrastructure failure, poor workmanship, or design), or human-caused threats (e.g., accidents, cyberattacks, political upheaval). The consequences associated with the vulnerabilities of a community, as a result of a hazard or threat being realized, is one way to measure the impacts associated with risks. Therefore, risk is defined in 1 by

$$\text{Risk} = \text{Consequence} \times \text{probability} \times \text{vulnerability}. \quad (1)$$

Resilience analysis includes both the time before (planning capability), during (absorbing capability), and after a disruption event occurs (recovery and adaptation capability), including the actions taken to minimize the system damage or degradation, and the steps taken to build the system back stronger than before. Figure 4a shows this timeline and the planning [15, 25, 35, 36, 61, 62, 85, 90],



**Fig. 4** (a) Resilience framework overview with and without the use of digital twins and (b) risk assessment adoption framework (modified from Crosby et al. 2020)

absorbing [15, 25, 61, 62, 65, 80, 85, 90], recovering [6, 78, 85, 90, 92], and adapting [7, 8, 15, 25, 78, 81, 85, 90, 92] phases of a resilience event. As shown in Fig. 4, the system initially is in a steady state. After the disruptive event occurs at  $t_d$ , the system’s performance starts decreasing and then a contingency plan is implementing at time  $t_c$ . Then, there are four “recovery” scenarios. In the first scenario (blue line), the performance of the system gradually recovers without any outside intervention until it reaches the original steady state. In the second scenario (purple, dashed line), the system first reaches a new steady state, but eventually returns to its originally state. For example, temporary routes and measures are taken to meet immediate needs of a community’s operations when the system is damaged due to an earthquake. However, it may take weeks or months for the system to fully recover. The worst scenario is when the system cannot recover (red dashed line). The last scenario is to reach the recovery state earlier by using a holistic digital



twin (DT) framework (green line), which will be discussed in the last section of this chapter. Figure 4b showcases a risk assessment adoption framework [21].

Seismic resilience is the evaluation of the post-earthquake functionality of structural systems that are critical for rescue and discovery [71], as well as the performance of the system after the damage has been mitigated [51]. Multiple seismic resilience frameworks have been proposed and implemented to evaluate the performance of aging structural systems [17, 18, 34, 39, 63, 64, 75]. The transportation system, electric power and water supply systems, acute-care hospitals, and organizations for emergency management are critical for communities, and seismic resilience frameworks have been proposed to alleviate the associated risks between these systems [14, 45, 53, 57, 91]. According to [48], these methods can be grouped into eight types: (1) resource-constrained modeling, (2) machine learning, (3) dynamic economic impact modeling, (4) system dynamics simulation, (5) agent-based simulation, (6) discrete-event simulation, (7) stochastic simulation, and (8) network modeling.

A system's performance can be measured by multiple metrics. Threats to the system can cause abrupt changes, which can either be gradual or disruptive. Community earthquake loss of resilience, with respect to a specific earthquake, can be quantified by measuring the expected degradation in quality (probability of failure) over time. This is mathematically expressed by [13] as

$$Loss = \int_{t_0}^{t_1} [100 - Q(t)] dt \quad (2)$$

where  $Q(t)$  is the quantified metric of community functionality,  $t_0$  is the time the earthquake begins, and  $t_1$  is the time the repair process finishes.

The normalized resilience index introduced by [17] is defined as

$$R = \int_{t_{OE}}^{t_{OE}+T_{LC}} \frac{Q(t)}{T_{LC}} dt \quad (3)$$

where  $T_{LC}$  is the control time that makes the resilience index,  $R$ , a dimensionless indicator. It is usually considered to be 50 years for residential buildings or the longest recovery time under the considered seismic intensities.

The values of  $R$  are in the range of  $[0, 1]$  and measure a community's seismic resilience. The higher  $R$  is, the more resilient the community is to earthquake hazards and the smaller the losses it has. However, a limitation of this indicator is that it only accounts for an earthquake of specific magnitude or intensity.

The loss function is then determined by the direct and indirect losses as [17]

$$L = L_D + (\alpha \times L_I) \quad (4)$$

where  $L_D$  and  $L_I$  are the direct and indirect losses, respectively, and  $\alpha$  is the weight factor that depends on the importance of structures to the society and their influence to other systems.

Loss	Equation	Vulnerability curve
Structural/ Non-structural component with k members	<p><b>Fragility curve</b> (Cimellaro et al., 2005)</p> $L_{DE,K}(I) = \frac{\sum_{k=1}^n W_k * L_{DE,K}}{N}$ <p>where <math>W</math> = weight factor with importance of structural/non-structural element in structure/building  <math>N</math> = total number of structural/non-structural members in a building</p> $L_{DE,K} = \sum_{j=1}^n \left[ \frac{C_{Sj}}{I_s} \prod_{i=1}^{t_i} \frac{1 + \delta_i}{1 + r_i} \right] P_j \{U_{i=1}^n (R_i \geq r_{lim,i})\}   I\}$ <p>Where <math>P_j</math> is the conditional probability of exceeding a performance limit state <math>j</math>, when an extreme event of intensity <math>I</math> occurs  <math>C_{sj}</math> is the building repairing costs related to a <math>j</math> damage state  <math>l_{sj}</math> is the replacement building costs related to a <math>j</math> damage state  <math>r_i</math> is the annual discount rate applied for the time interval in years between initial investment and the extreme event  <math>\delta_i</math> is the annual depreciation rates</p>	<p><b>Vulnerability curve</b></p> $L_{DE,K} = \sum_{j=1}^n \left[ \frac{C_{Sj}}{I_s} \prod_{i=1}^{t_i} \frac{1 + \delta_i}{1 + r_i} \right] Damage (\%)$ <p>Where <math>C_{sj}</math> is the building repair costs  <math>l_{sj}</math> is the replacement building costs  <math>r_i</math> is the annual discount rate applied for the time interval in years between initial investment and the extreme event  <math>\delta_i</math> is the annual depreciation rate                  Damage (%) is the percentage obtained from the vulnerability curve</p>
Casualties	$L_{DC}(I) = \frac{N_{in}}{N_{tot}}$ <p>Where <math>N_{in}</math> = number of fatally and non-fatally injured  <math>N_{tot}</math> = number of occupants in a building</p>	
Total direct losses	$L_D = (L_{DE})^{a_{DE}}(1 + a_{DC}L_{DC})$ <p>Where <math>a_{DE}</math> = weighting factor related to construction losses  <math>a_{DC}</math> = weighting factor related to the nature of occupancy</p>	
Total indirect losses	$L_I = (L_{IE})^{a_{IE}}(1 + a_{IC}L_{IC})$ <p>Where <math>a_{IE}</math> = weighting factor related to construction losses in business interruption  <math>a_{IC}</math> = weighting factor related to the nature of occupancy</p>	

Fig. 5 Summary of direct and indirect earthquake losses with their respective equations

Direct losses of earthquakes refer to instant, quantifiable losses during a disaster, such as the number of fatalities or injuries and replacement or repair costs of damaged structures.

A summary of direct and indirect losses is illustrated in Fig. 5.

There are also important considerations when calculating the total losses. This is the rate of asset value depreciation [66]. The depreciation of a building is the process of methodically deducting the documented cost of the building from its current value until its value is either zero or is no longer worth salvaging the building. The annual rate of depreciation varies depending on the type of building being depreciated. The annual rate of depreciation for popular building types is summarized in Fig. 6. Furthermore, the yearly rate of depreciation can be calculated as the reciprocal of the asset’s useful life.

### Seismic Resilience Properties

Seismic resilience consists of the following properties:

**Rapidity** The capacity to meet priorities and achieve goals in a timely manner in order to contain losses, recover functionality, and avoid future disruption. Mathematically, it represents the slope of the functionality curve (Fig. 7) during the recovery time and can be expressed by the following equation:

Rate of depreciation (%)	Type of building
5	Buildings that are utilized exclusively for residential purposes, with the exception of boarding houses and hotels, are referred to as residential premises. It is only when more than 66.66% of a building’s built-up floor space is used for residential purposes that the structure is considered as residential.
10	All other building types do not belong into the category of residential buildings.
100	Buildings utilized for the installation of machinery and plants that are integral to the water treatment system and water supply system.

Fig. 6 Summary of rates of depreciation for various building types [66]

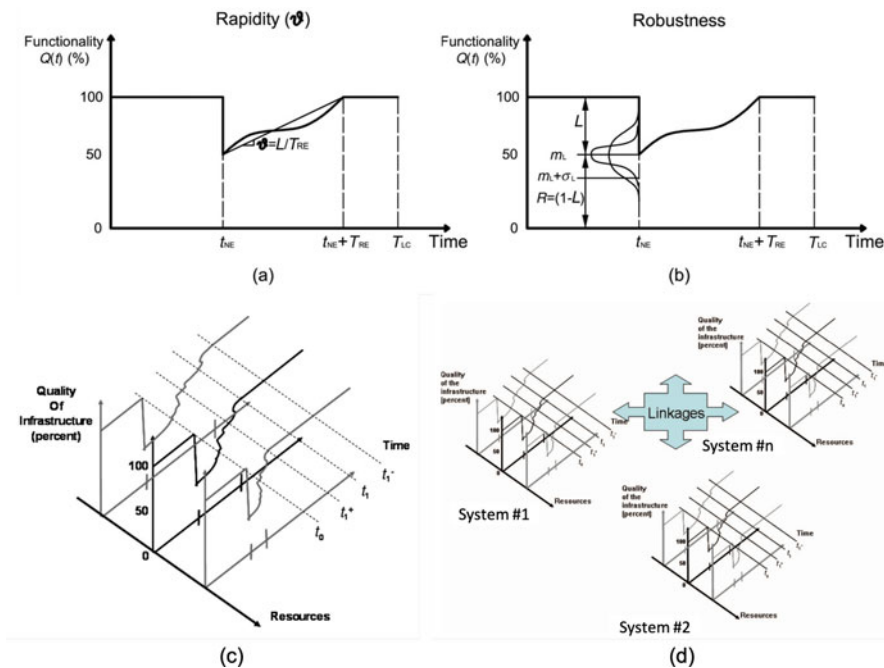


Fig. 7 Dimensions of resilience: (a) rapidity, (b) robustness, (c) resourcefulness, and (d) redundancy [18]

$$Rapidity = \frac{dQ(t)}{dt} \text{ for } t_{OE} \leq t \leq t_{OE} + TRE \tag{5}$$

An average estimation of rapidity can be defined by knowing the total losses and the total recovery time to again reach 100% functionality.

*Robustness* Strength, or the ability of elements, systems, and other measures of analysis to withstand a given level of stress or demand, without suffering degradation or loss of function. It is therefore the residual functionality right after the extreme event (Fig. 7b) and can be represented by

$$\text{Robustness}(\%) = 1 - L(m_L, \sigma_L) \quad (6)$$

where  $L$  is a random variable expressed as a function of the mean  $m_L$  and the standard deviation  $\sigma_L$ .

A possible way to increase uncertainty in the robustness of the system is to reduce the dispersion in the losses represented by  $\sigma_L$ .

*Redundancy* Is the extent to which alternative elements, systems, or other measures exist, which are substitutable, that is, capable of satisfying functional requirements in the event of disruption, degradation, or loss of functionality. In Fig. 7d, a network of systems is illustrated. In this case, we consider the simplest scenario, where the performance of each individual system will be aggregated to the overall performance of the network. We will elaborate on some more complex models in the section that follows.

*Resourcefulness* Is the capacity to identify problems, establish priorities, and mobilize alternative external resources when conditions exist that threaten to disrupt some element, system, or other measure. Resourcefulness can be further conceptualized as consisting of the ability to apply material (i.e., monetary, physical, technological, and informational) and human resources in the process of recovery to meet established priorities and achieve goals. Resourcefulness is primarily an ad hoc action, which requires momentary decisions to engage additional and alternative resources. In Fig. 7c, a third axis shows that additional resources can be used to reduce the time to recovery. Theoretically, if there were infinite resources available, the time to recovery would asymptotically approach zero, but even in the presence of enormous financial and labor capabilities, human limitations will necessitate a practical minimum time to recovery. In fact, even in a resourceful society, the time to recovery after a disaster may be significantly longer than necessary due to adequate planning, organizational failures/inadequacies, or ineffective policies. On the contrary, in a less technology advanced society, where resources are scarce, time to recovery lengthens, approaching infinity in the absence of any resources (Fig. 8).

There are four resilience dimensions: technical, organizational, social, and economic [13]. Each dimension is analyzed below:

1. The *technical* dimension corresponds to the capacity of the structural/physical systems to perform at acceptable levels when subject to earthquakes.
2. The *organizational* dimension corresponds to the capacity of organizations that manage critical facilities to make decisions and react toward achieving the resilience properties: robustness, redundancy, resourcefulness, and rapidity, as explained above.

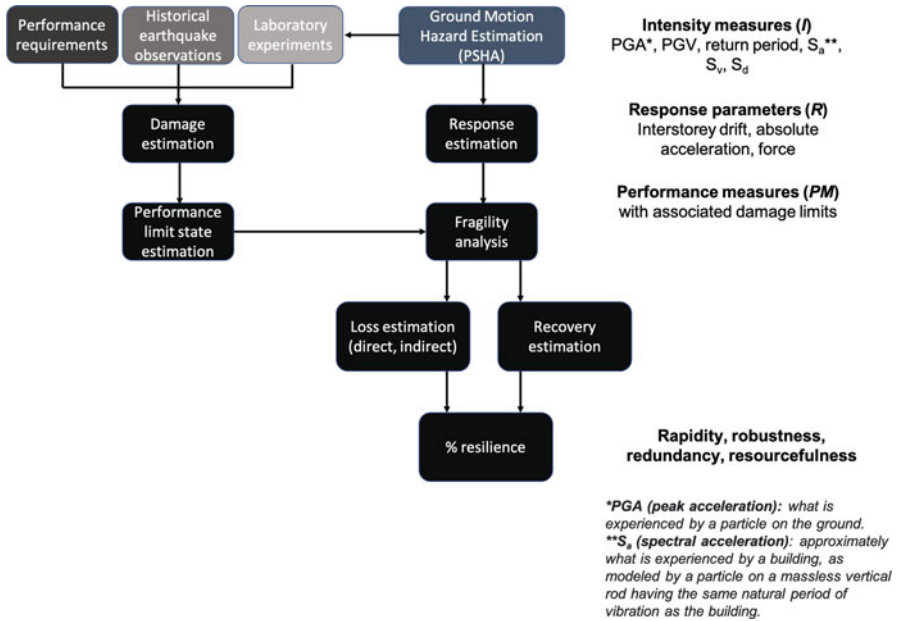


Fig. 8 Performance assessment methodology (MCEER approach) [17]

3. The *social* dimension refers to government measures undertaken to mitigate the damages and loss of critical services induced by earthquakes.
4. The *economic* dimensions refers to the capacity to mitigate both direct and indirect economic losses induced by earthquakes.

These four dimensions of community resilience—technical, organizational, social, and economic (TOSE)—as defined by [13] cannot be addressed by a single metric. Instead, multiple metrics need to be taken into consideration in all the interrelated resilience dimensions.

Figure 9 links the four TOSE dimensions to key infrastructure assets: power, water, hospital, and local emergency management systems.

### Seismic Risk Assessment Tools

**HAZUS.** Initially used as mitigation tool, HAZUS has been increasingly deployed for response and recovery. HAZUS assesses a variety of hazards, including hurricane wind, riverine and coastal floods, earthquakes, and tsunamis. This tool relies on a strong multidisciplinary coordination. Engineers, seismologists, geologists, and social scientists collaborate with decision-makers to provide a comprehensive risk assessment (from mitigation strategies to inventory modeling). Additionally, HAZUS relies on nationwide databases and is used for preparedness exercises

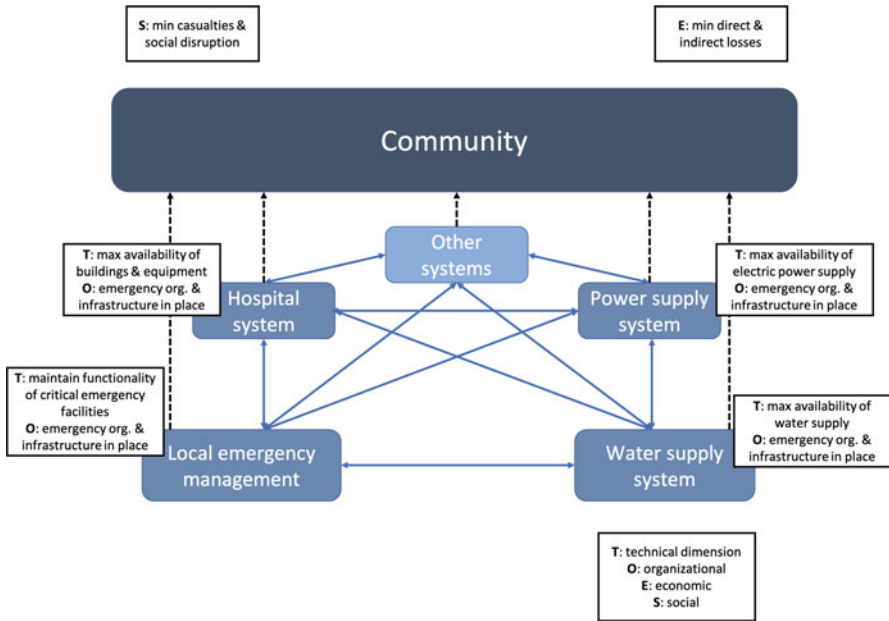


Fig. 9 Community dimensions of resilience as adopted by [13]

in the United States. International applications are also worth mentioning; for example, a collaborative study that was carried out in Egypt with the National Research Institute of Astronomy and Geophysics (NRIAG). The disaster response information timeline is of particular relevance as it points to one of the most critical aspects of crisis communication management: when and how decision-makers should be informed. When, for example, an earthquake occurs, the preliminary HAZUS models are run after 45 minutes. After the first hour, significant information (e.g., buildings, casualties, debris, shelter needs) is shared in a dashboard. An update on losses and products (e.g., utilities and essential facilities) is provided two hours after the event when additional data is available.

**CAPRA** is a fully probabilistic and peril-agnostic risk assessment system. Overall, the CAPRA initiative aims at developing both risk assessment and communication tools to

1. Guide decision-makers about the potential impact of disasters associated with natural hazards
2. Formulate comprehensive disaster risk management strategies at subnational, national, and regional levels
3. Develop a common, open, and modular methodology to assess and quantify disaster risk from multiple perils
4. Provide access to state-of-the-art fully probabilistic hazard and risk assessment
5. Tools to local institutions, mainly needed in developing countries

6. Develop a flexible methodology in which updates and improvements can be incorporated by universities, research centers, etc.

Although originally developed for disaster risk management (DRM) and disaster risk reduction (DRR) planning activities, CAPRA's risk assessment tools can be used for rapid post-event damage and loss assessments at different scales depending on information availability, having been tested with events in Asia, Europe, and Latin America.

The **PAGER (Prompt Assessment of Global Earthquakes for Response)** system developed by the USGS constitutes a prime example of robust tools used for loss and damage estimation [37, 76]. Updated ground-motion maps are provided by the USGS ShakeMap system immediately after an earthquake occurs. This tool estimates potential casualties and economic losses due to country-specific vulnerability and loss models based on global population databases and exposed people to a given macroseismic intensity level. In developing countries, the approach is empirical, whereas in highly developed countries, the availability of building codes allows the use of analytical models and semi-empirical solutions.

**ShakeCast** ([44]) (<http://usgs.github.io/shakecast>) is a similar fully automated open-source system using ShakeMap input, and HAZUS methodology [28]. Although HAZUS is used as the default methodology, the users can also define the input such as fragility curves for buildings, bridges, to name a few. Shake-maps are applied to a list of critical and industrial facilities and the probability of damage is estimated based on fragility curves. Alerts are sent on a web interface and communicated via emails and texts to registered end-users in order to be used for prioritizing inspection (green, yellow, orange, or red).

The **Global Disaster Alert and Coordination System (GDACS)** ([www.gdacs.org](http://www.gdacs.org)) is a framework developed in collaboration between the United Nation and the European Union. It has data and tools from several organizations: JRC (Joint Research Center of the European Commission) and INFORM (Index for Risk Management), NEIC (National Earthquake Information Center) and USGS, OCHA (UN Office of Coordination of Humanitarian Affairs), and INGV. The data (earthquake magnitude, depth, location, population within 100 km, vulnerability) is obtained via web services at 5 min intervals and a qualitative three-level alert is issued (green, orange, or red) based on the extent of the event (earthquake or other natural hazard) and the ability of the country to address it.

SeisDaRo 3 [69] is a near-real-time system based on the PAGER methodology and the SELENA module. It is directly connected to a custom shake-map system (based on the ShakeMap v3.5 approach), and users can visualize loss maps by running the system's modules in less than 6 min. The process is as follows: (1) global loss statistics from the event are generated from the PAGER methodology and (2) a more detailed account of the earthquake's impact is presented within a few minutes using the SELENA algorithm to estimate damages and losses. SELENA [49] is a capacity spectrum-based method, where the vulnerability is computed based on the spectral parameters (accelerations and displacements), and the ground-motion estimates are provided using deterministic or probabilistic



analysis, including site effects. The uncertainties are calculated via a logic tree and a Monte Carlo approach.

**ELER** is operational in the Istanbul area and uses the shake-maps generated by KOERI/RETMC, which are available within a few minutes after the event [93]. The damage and loss are calculated based on a grid, in addition to the shake-map, exposure, and vulnerability data. The grid-based building inventory was initially generated by using the 2000 Turkish Statistical Institute (TUIK) Building Census (including information on the construction year, number of floors, and building construction type and the demographic data). Then, a district-based building inventory of Istanbul was performed to update the TUIK statistics, and the final inventory was finalized into  $0.005^\circ$  grids by using 2008 building line geometries of 1/1000-scaled existing maps. The building damage is evaluated using the ELER methodology, and the loss is estimated using the HAZUS-MH methodology [28].

The BRGM (French Geological Survey) has developed a rapid response assessment system (**SEISAID**) based on the PAGER approach [3, 4]. The tool generates rapid shaking estimates, and it projects population density data on seismic intensity levels, similarly to the PAGER approach. It allows to rapidly estimate the number of casualties and homeless people. The relation between the macroseismic intensity and the human losses is used to calibrate data from past French earthquakes and from most seismic scenarios.

The following assessment tools are not based on shake-maps. They either simulate specific earthquake scenarios without accounting for field observations or they directly estimate losses from the earthquake's parameters.

The ICES Foundation (<http://www.icesfoundation.org/Pages/QLarmEventList.aspx>) developed the **QLARM** software [70], which provides loss estimates within less than 24 h after a potentially damaging earthquake occurs worldwide. This is achieved in partnership with the Swiss Seismological Service and alerts users with the number of fatalities and the average damage of buildings. The ground shaking is estimated for each population settlement using the earthquake characteristics and soil characteristics of each region ( $V_{s,30}$  map). The damage estimation is obtained using empirical relations derived from 1000 earthquakes with known losses. The software also provides evaluations of the percentage of the population belonging to classes of vulnerability (definition of the classes based on the building type) including time variance of population distributions. It also provides the percentage of buildings in each of the five defined damage states, as well as the number of fatalities and injured people in each settlement.

The Department of Civil Protection (DPC) has developed an Information System for Emergency Management (**SIGE-DPC**) to identify the characteristics of an earthquake event and estimate an expected distribution of structural damage and human casualties [54]. However, the shake-map is not used, which means measured or observed ground shaking is bypassed and intensity maps are not updated. The European Centre for Training and Research in Earthquake Engineering (EUCENTRE) has developed web-based GIS tools to measure near-real-time damage for a wide range of exposed assets and systems, such as residential buildings [26], schools [9, 10], port infrastructure [11], road networks [24], or airports [12].



**EQIA** is an Earthquake Qualitative Impact Assessment [31], which provides fast and automatic damage assessment for crustal earthquakes that have a magnitude 5 or higher worldwide. It provides a range of potential impacts (based on intervals of potential fatalities), in order to rate the severity of the event that triggers rapid actions. They have developed two empirical equations; a GMM for the estimation of impacted areas, and an equation regarding the number of fatalities to the earthquake magnitude and the population density. This approach has the merit of bypassing the shake-map step and of providing a direct impact estimate with limited input data. For large earthquakes of magnitude 7 or higher, the source is modeled as a 1D finite rupture, and different assumptions regarding the position of the fault and its nodal plane are taken into account, adding up to the uncertainties of the earthquake scenario. Julien-Laferriere [38] conducted a comparative study between EQIA predictions on past earthquakes and their actual impacts, which showcased satisfactory performance by EQIA. Currently, EQIA outcomes are not made publicly available; however, a group of selected end users has access or when prompted by governmental organizations (e.g., French civil protection).

The Taiwanese system **TELES (Taiwan Earthquake Loss Estimation System [86])** is based on the HAZUS methodology and provides decision support after strong earthquakes. The earthquake data comes from the Central Weather Bureau networks, and the parameters (location, magnitude) are given by TREIRS (Taiwan Rapid Earthquake Information Release System) within 90 sec after the earthquake event. This enables the estimation of ground motion parameters (such as PGA and PGV) from a scenario earthquake as well as prediction equations. The liquefaction effects are also considered and a probability of damage state for 15 different types of buildings is provided with the use of analytical methods. Damage maps and tables are automatically generated within 3–5 min after receiving the earthquake alert signal. This procedure does not seem to integrate the new Taiwanese shake-map system yet.

Two other systems are available in Japan: the **READY** system [47] and the **SUPREME** system [60] for possible damages to gas infrastructure assets. **READY** is a system with an associated array of strong motion accelerometers and borehole systems for liquefaction monitoring. The stations are connected to observation centers via high-speed telephone lines and satellites as a backup. The intensity map is immediately generated after an earthquake event, along with other useful information such as hospital or shelter locations. The **SUPREME** system uses Spectrum Intensity Sensors in order to evaluate damages on critical gas pipes. The response spectra are evaluated in the range 0.1–2.5 sec, and if the spectral intensity becomes greater than 30–40 cm/s, the decision to shut down the gas supply is made.

The **ISARD** system, a collaborative project between France, Spain, and the principality of Andorra [32], has been used in operational mode since 2007 by the civil protection of Catalonia, Spain. This system performs rapid loss assessment by coupling a rough estimate of the seismic intensity properties using an intensity prediction equation (IPE), with a loss model similar to that described by [59]. The result is sent for validation by SMS to an on-call seismologist in less than 10 min.

Then, the seismologist sends reports to civil protection via SMS and e-mails through this system.

A summary of the rapid damage and loss assessment systems is presented in Fig. 10, with the required input data and the output format of each system.

## 2 Overview of Macroscopic Earthquake Management Approaches

Three models of recovery functions are considered at the community level as proposed by [18]. Those are analyzed below and illustrated in Fig. 11:

1. Linear recovery, which is used when no information is available related to the community preparedness, resource availability, and societal response.
2. Exponential recovery, which is used when there is an initial flow of resources, but then the rapidity of recovery decreases as the process nears its end.
3. Trigonometric recovery, which is adopted when there is a lack of either organization or resources. After the community is organized (e.g., with the help of other communities), then the recovery phase starts and the rapidity of recovery increases.

You et al. [88] proposed a framework to assess the seismic resilience of a community with the assumption that seismic performance parameters (SPPs) of buildings, such as their collapse capacity, repair cost, repair, time to name a few, are known. The framework is schematically presented in Fig. 12.

Maroufi and Borhani [46] proposed a framework to evaluate the community resilience in Mashhad city in Iran. They employed 23 indicators as illustrated in Fig. 13. A comprehensive list of performance indicators is provided by [46]. Readers can refer to [87] for an inventory of community seismic resilience studies.

## 3 Overview of Microscopic Earthquake Management Approaches

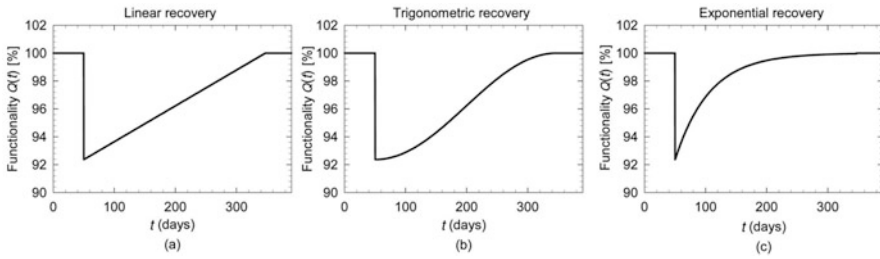
Recently, seismic planners and policymakers have focused on achieving “better than code” seismic design and develop guidelines to estimate building downtime.<sup>2</sup> The Federal Emergency Management Agency (FEMA) defines “functional recovery” of a building as its performance state, where it maintains its ability to perform at its intended use [58]. Both FEMA and the National Institute of Standards of Technology (NIST) develop performance objectives related to post-earthquake

---

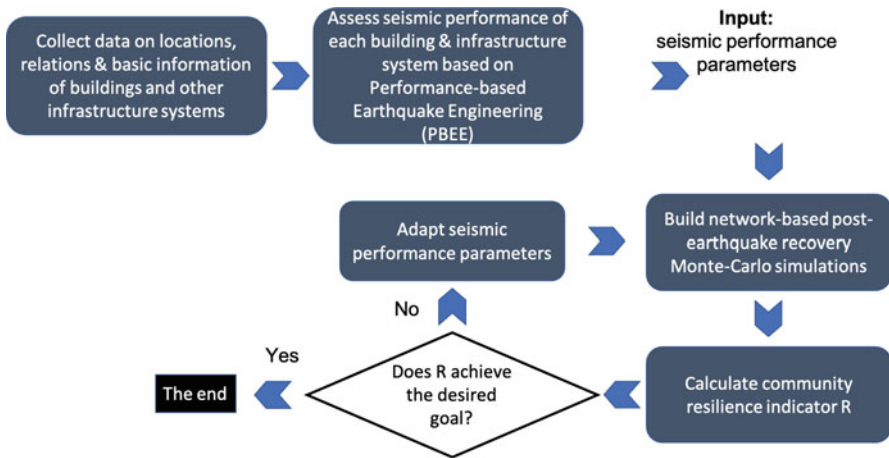
<sup>2</sup> Building downtime is defined as the time required to achieve a recovery state after an earthquake [50].

Seismic assessment tool	Inputs	Outputs	Scale	End users
PAGER	Shake-map & empirical/analytical vulnerability assessment	Fatalities & economic losses & uncertainty quantification	Wholistic earthquake approach	Open-source
ShakeCast	Shake-map & facility inventory	Shaking values & inspection prioritization, email/text alerts	At the level of individual facilities	Restricted to registered users (e.g., infrastructure managers)
GDACS	PAGER output	3-level color alert	Wholistic earthquake approach	Open-source
SeisDaRo	Custom shake-map & building inventory & vulnerability data	Fatalities graphs & exposure tables, fast global damage estimates	At the level of cities/municipalities	Restricted to authorized users only
ELER	Shake-map & building inventory & occupancy/population database	Damage & loss maps	At the level of a city district/large building block	Restricted to authorized users only
SEISAID	Shake-map & building inventory & occupancy/population database	Collapsed dwellings & injuries	Wholistic earthquake approach	Restricted to authorized users only
QLARM	Scenario earthquake & empirical relations	Fatalities & average damage on buildings on global scale	Wholistic earthquake approach	Restricted to authorized users only
SIGE-DPC	Earthquake characteristics & empirical relations	Collapsed dwellings, unusable dwellings, fatalities & homeless	At the level of cities/municipalities	Restricted to authorized users only
EQIA (ESMC)	Earthquake characteristics & population density (LandScan)	Global impact estimate	Wholistic earthquake approach	Under development & validation
TELES	Earthquake scenario & liquefaction effects	Damage maps & tables	At the level of a city district	?
READY	Intensity map	Damages on roads & buildings, inaccessible roads	At the level of a city district/large building block	?
SUPREME	Spectral intensity	Damage on gas pipes	At the level of facilities (e.g., buried pipelines)	Restricted to gas operators only
ISARD	Earthquake characteristics & empirical relations	Collapsed dwellings, unusable dwellings, fatalities & homeless	At the level of cities, municipalities	Restricted to civil protection

Fig. 10 Seismic risk assessment tools with their input, output data sources (Adapted by [33])



**Fig. 11** Functionality curves representing an (a) average-prepared community, (b) not well-prepared community, and (c) well-prepared Community (Adapted by [18])



**Fig. 12** Resilience framework linking long-term resilience indicator to seismic performance of individual buildings (Adapted from [88])

recovery times (REF) [19, 74]. For example, FEMA P-2082 recommends assigning target recovery times to every new building based on the building’s risk category [27]. Similarly, the San Francisco Planning and Urban Research Association (SPUR) has identified target recovery times for a resilient San Francisco [55].

Multiple frameworks and assessment tools have been developed to evaluate the post-earthquake recovery time of buildings. Figure 14 summarizes the most widely used assessment tools.

A summary of REDi and FEMA P-58 resilience objectives is illustrated in Figs. 15 and 16.

Earthquake damage varies based on the level of shaking and characteristics of the structural building components. Basic retrofitting includes buildings in areas of Risk Category IV (e.g., hospitals, emergency vehicles, fire stations). Buildings designed with the new-code have very low-casualty risks in the United States, with design choices affecting the amount of time required before a building can be occupied after an earthquake. More resilient buildings typically cost slightly more upfront, but result in lower post-earthquake repair costs and consequences.

Resilience dimension	Indicators
Economic (occupation, housing capital, financial capital, economic diversity)	<ul style="list-style-type: none"> <li>• % of employed population</li> <li>• % of home ownership</li> <li>• Number of construction licenses issued by the district municipality in the last fiscal year</li> <li>• Ratio of large to small business</li> </ul>
Socio-economic (population exposure to hazard, education level, age, special needs)	<ul style="list-style-type: none"> <li>• Number of habitants per 1,000 square meters</li> <li>• % of the population within high-risk zones</li> <li>• % of people with higher education level</li> <li>• % of population aged between 6 and 65</li> <li>• % of people with physical or mental disabilities</li> </ul>
Environmental (exposure, vegetation, vulnerability of place)	<ul style="list-style-type: none"> <li>• % of the areas with a slope of more than 4% in the neighborhood</li> <li>• Natural or green areas per capita</li> </ul>
Organizational/managerial (resources, managerial qualifications, managerial process)	<ul style="list-style-type: none"> <li>• Municipal budget line of each district for crisis management and prevention</li> <li>• Number of emergency management maneuvers</li> <li>• Number of neighborhood emergency response volunteers per 1,000 people</li> </ul>
Physical/Infrastructure (physical capital, infrastructure capital, physical exposure to hazard)	<ul style="list-style-type: none"> <li>• % of the deteriorated urban fabric</li> <li>• Number of healthcare centers per 1,000 residents</li> <li>• Number of emergency shelters per 1,000 people</li> <li>• % of critical infrastructure located inside high-risk areas</li> </ul>
Cultural/community competence (social trust, religious ties, cultural features, community participation, public satisfaction)	<ul style="list-style-type: none"> <li>• Inhabitants' perception of social trust</li> <li>• Number of religious-based centers per 1,000 residents</li> <li>• Number of phone calls to public relation centers of each subcity district per 1,000 residents</li> <li>• Inhabitants' satisfaction towards life</li> <li>• % of satisfaction from local councils</li> </ul>

**Fig. 13** Functionality curves representing an (a) average-prepared community, (b) not well-prepared community, and (c) well-prepared Community (Adapted by [18])

Molina Hutt et al. [50] address delay factors that impede the initiation of repairs such as post-earthquake inspection, stabilization, engineering mobilization and review, permitting, contractor mobilization, and financing. If a building does not experience damage, then the delay estimate will be zero (Fig. 17).

**Building Robustness** The National Earthquake Hazards Reductions Program [52] provisions propose a “function loss” performance metric that requires all buildings in risk category IV to have a probability of 10% or less of not being operational after a “functional-level earthquake,” which roughly corresponds to ground motion intensity with a return period of 475 years.

Performance Assessment Tool	Framework Description	Limitations
FEMA P-58	<p>Translates engineering demand parameters for individual buildings (e.g., story drifts and floor accelerations) to performance metrics (e.g., casualties, economic loss and repair time) using fragility functions and Monte Carlo simulations to account for uncertainties in structural response parameters</p>	<ul style="list-style-type: none"> <li>• Only considers repair time for full recovery, intermediate recovery states are not considered</li> <li>• Only repairs in series (one floor at a time) or parallel (all floors are repaired simultaneously)</li> <li>• Does not account for delays of repair initiations due to contractor mobilization or financing</li> </ul>
REDi	<ul style="list-style-type: none"> <li>• enhanced FEMA P-58 by estimating repair initiation delays between the start of an earthquake and start of repairs and estimating utility description (e.g., electrical, water systems)</li> <li>• Propose 3 post-earthquake recovery states:                             <ul style="list-style-type: none"> <li>➤ Reoccupancy (building is safe enough to occupy)</li> <li>➤ Functional recovery (basic building functionality restored)</li> <li>➤ Full recovery (building is restored to its pre-earthquake condition)</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Conservative reoccupancy criteria (e.g., all structural, plumbing and HVAC component repairs should be completed before a building is occupied)</li> <li>• FEMA P-2055 (2019) and SPUR (2012) recommends habitability if the building does not pose a life-safety risk</li> </ul>

**Fig. 14** Comparison between performance assessment tools for individual buildings and their limitations

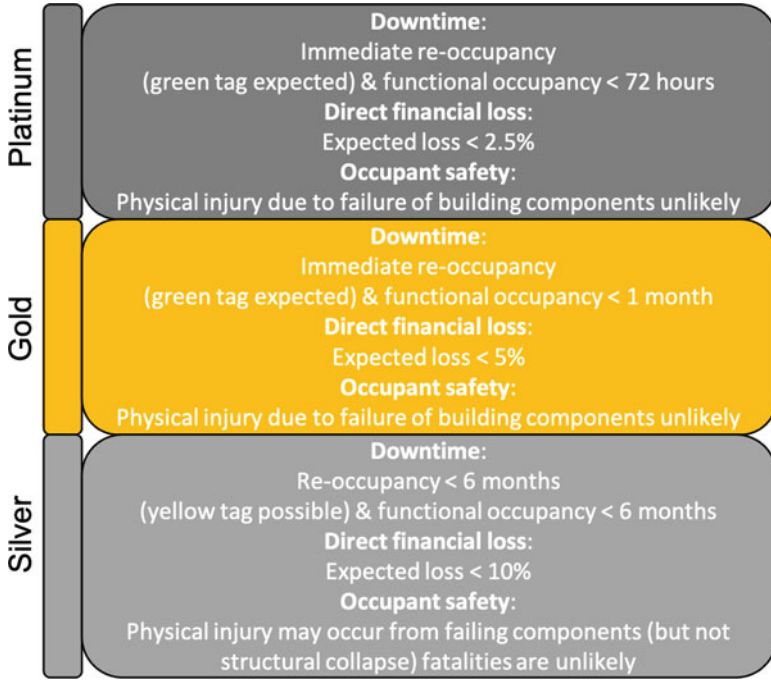


Fig. 15 Summary of REDi resilience objectives [1]

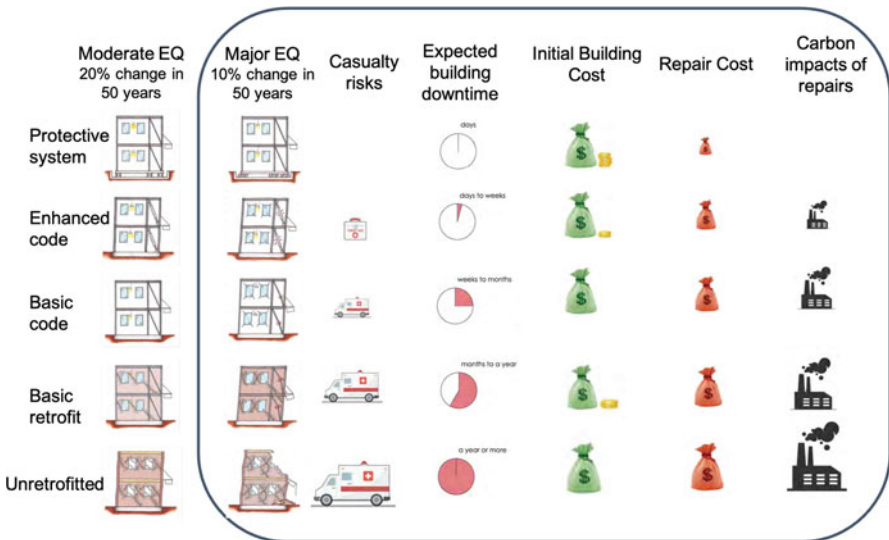
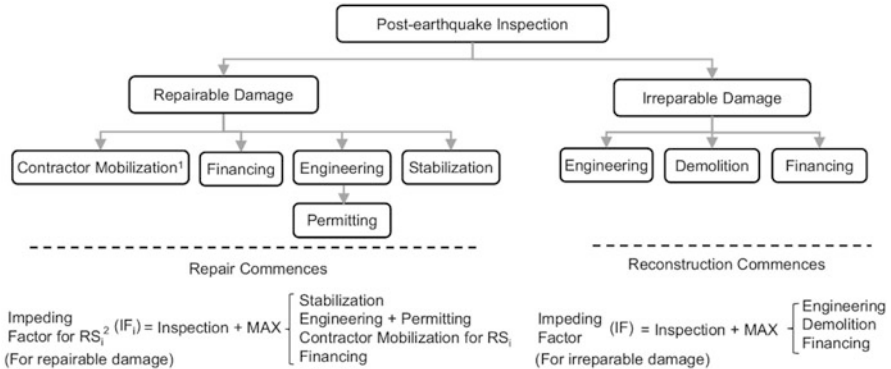


Fig. 16 Summary of FEMA P-58 resilience objectives





<sup>1</sup> Contractor mobilization delays are estimated for each repair sequence (RS)  
<sup>2</sup> Subscript 'i' indicates that the delay can vary for each repair sequence

Fig. 17 Sequencing of impeding factor delays [50]

**Rapidity** FEMA P-2082 [27] recommends assigning target functional recovery downtimes (ranging from hours to months) to every new building, depending on the building’s risk category. Poland [55] requires all residences to be repaired within a 4-month period of an earthquake representative of a 475-year intensity-level event.

Methodical collection of historical data after earthquakes about the degree of damage to buildings and the time required to achieve each phase of recovery is needed to validate and refine the assumptions of existing frameworks such as FEMA P-58 and REDi.

## 4 Discussion and Conclusions

Earthquakes are complex loads to a structure. Apart from the implementation of design codes (e.g., Eurocode 8), various novel building damage evaluation techniques and retrofitting strategies can be employed to improve or accelerate the infrastructure’s recovery. Retrofitting an existing building is usually preferred compared to constructing a new building due to its cost-effectiveness. The decision-makers, designers, or stakeholders prefer to select the retrofitting strategy with the maximum resiliency and the minimum cost.

When it comes to the resiliency of a community, each subsystem should be considered with multidisciplinary and multicriteria methodologies. Resiliency models in those cases need to evaluate economic, technical, organizational, and social aspects of a community.



The post-earthquake retrofitting practices adopted in numerous European countries reveal that energy efficiency and seismic vulnerability aspects have not been addressed in a unified framework following the corresponding standards/guidelines. Despite the increasing awareness about sustainability issues associated with the existing building stock, it is a matter of fact that major retrofit plans were undertaken only in the aftermath of devastating earthquakes [23].

The review of existing seismic assessment tools reveals that real-time updates on shake-maps are challenging for the estimation of the actual fault geometry, site amplification factors (such as soil conditions), and the choice of GMM models in areas where they are not available. Data collection is another challenge; however, data mining through social media (e.g., Twitter feeds [2]) can be efficient due to the reactivity of users right after an earthquake occurs.

Systems such as PAGER, GDACS, or EQIA provide a holistic overview of the potential impact of an earthquake. These tools can rapidly size a disaster and decide the level (e.g., regional, national, international) at which crisis management operations need to be activated as well as aid and resources to be allocated. However, first respondents need to have a more detailed view at a local level (e.g., at which street and building block rescue teams are needed). In these cases, systems that estimate damages at a lower level of detail (e.g., SeisDaRo, ELER, SEISAID) provide reliable results to meet these operational needs. Therefore, the coupling of a shake-map system and a rapid loss assessment tool, which can be achieved via a digital twin implementation (e.g., at a city district level) is a suggested approach; shake-maps provide accurate ground motion prediction estimates, which feed fragility models of various structural types.

None of the current systems have been deployed on critical facilities and further research efforts need to be undertaken to validate promising preliminary results [29]. Better quantifying human impacts is another research direction that needs to be further considered. Currently, human impacts are estimated based on simplified, empirical methods. For instance, they either directly apply predefined loss rates to resident population according to the seismic intensity (PAGER) or propagating predicted building damages to occupants (SIGE, SEISAid, ISARD). Dynamic population changes (e.g., accounting for hourly pendulum movements) and seasonal changes (e.g., accounting for tourist populations) is a noteworthy consideration for future research.

New technologies such as laser scanning, unmanned aerial vehicles (UAVs), computer vision (i.e., automated damage identification), and digital twins offer a plethora of opportunities for improving the current approaches. For instance, [43] use UAVs to map a building and pre-earthquake structural analysis to predict a building's post-earthquake response. The opportunity digital twins offer to simulate scenarios can be helpful toward predicting structural damage a priori. Currently, there have been a few researchers predicting the post-earthquake capacity of buildings using deep learning networks in simplified scenarios [68, 89].

## References

1. ARUP: Redi rating system: Resilience-based earthquake design initiative for the next generation of buildings, Version 1.0 (2013). <https://www.redi.arup.com/>
2. Auclair, S., Boulahya, F., Birregah, B., Quique, R., Ouaret, R., Soulier, E.: Suricate-nat: Innovative citizen centered platform for twitter based natural disaster monitoring. In: 2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), pp. 1–8. IEEE (2019)
3. Auclair, S., Monfort, D., Colas, B., Langer, T., Bertil, D.: Outils de réponse rapide pour la gestion opérationnelle de crises sismiques. In: Colloque SAGEO (2014)
4. Auclair, S., Monfort, D., Colas, B., Langer, T., Perrier, P.: Evaluation rapide des bilans matériels et humains: une aide essentielle à la gestion opérationnelle des crises sismiques. In: 9ème Colloque National AFPS 2015 (2015)
5. Baker, J., Bradley, B., Stafford, P.: Seismic Hazard and Risk Analysis. Cambridge University Press, Cambridge (2021)
6. Bao, D., Zhang, X.: Measurement methods and influencing mechanisms for the resilience of large airports under emergency events. *Transp. A Transp. Sci.* **14**(10), 855–880 (2018)
7. Berkes, F., Ross, H.: Community resilience: toward an integrated approach. *Soc. Nat. Resour.* **26**(1), 5–20 (2013)
8. Boon, H.: Investigation rural community communication for flood and bushfire preparedness. *Aust. J. Emerg. Manag.* **29**(4), 17–25 (2014)
9. Borzi, B., Di Meo, A., Faravelli, M., Fiorini, E., Onida, M.: Definizione di un a procedura di prioritizzazione per interventi di mitigazione del rischio degli edifici scolastici. In: XIV Convegno L’Ingegneria Sismica in Italia ANIDIS (2011a)
10. Borzi, B., Di Meo, A., Faravelli, M., Fiorini, E., Onida, M.: Mappe di rischio sismico e scenario per gli edifici scolastici italiani. In: XIV Convegno L’Ingegneria Sismica in Italia ANIDIS (2011b)
11. Bozzoni, F., Lai, C.G., Marsan, P., Conca, D., Fama, A.: Webgis platform for seismic risk assessment of maritime port systems in italy. In: Proc., 4th PIANC Mediterranean Days Congress (2018)
12. Bozzoni, F., Ozcebe, A.G., Balia, A., Lai, C.G., Borzi, B., Nascimbene, R., Ippoliti, L., Berardi, S., Trombetti, M., Moroni, C.: Seismic ground response analyses at an international airport in northern italy by using a stochastic-based. *J. Theor. Appl. Mech.*, 58 (2020)
13. Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O’Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A., Von Winterfeldt, D.: A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra* **19**(4), 733–752 (2003)
14. Chen, C., Xu, L., Zhao, D., Xu, T., Lei, P.: A new model for describing the urban resilience considering adaptability, resistance and recovery. *Safety Sci.* **128**, 104756 (2020)
15. Chen, W., Li, J.: Safety performance monitoring and measurement of civil aviation unit. *J. Air Transp. Manag.* **57**, 228–233 (2016)
16. Chiou, B.S.-J., Youngs, R.R.: Update of the chiou and youngs nga model for the average horizontal component of peak ground motion and response spectra. *Earthquake Spectra* **30**(3), 1117–1153 (2014)
17. Cimellaro, G.P., Reinhorn, A.M., Bruneau, M.: Framework for analytical quantification of disaster resilience. *Eng. Struct.* **32**(11), 3639–3649 (2010a)
18. Cimellaro, G.P., Reinhorn, A.M., Bruneau, M.: Seismic resilience of a hospital system. *Struct. Infrastruct. Eng.* **6**(1-2), 127–144 (2010b)
19. Congress: In: National Earthquake Hazards Reduction Program Reauthorization Act of 2018: 115th Congress (2018)

20. Cornell, C.A.: Statistical analysis of maximum magnitudes. *Earthquakes Stable Continental Regions* **1**, 5–1 (1994)
21. Crosby, M., Steinle, M., Nobel, K., Smith T.: Airport security vulnerability assessments. Program for Applied Research in Airport Security, National Safe Skies Alliance, Inc. Sponsored by the Federal Aviation Administration (2020)
22. Daniell, J.E., Khazai, B., Wenzel, F., Vervaeck, A.: The CATDAT damaging earthquakes database. *Nat. Hazards Earth Syst. Sci.* **11**(8), 2235–2251 (2011)
23. Di Ludovico, M., Digrisolo, A., Moroni, C., Graziotti, F., Manfredi, V., Prota, A., Dolce, M., Manfredi, G.: Remarks on damage and response of school buildings after the central Italy earthquake sequence. *Bull. Earthquake Eng.* **17**(10), 5679–5700 (2019)
24. Di Meo, A., Borzi, B., Quaroni, D., Onida, M., Pascale, V.: Real time damage scenario and seismic risk assessment of Italian roadway network. In: 16th European Conference on Earthquake Engineering, Thessaloniki, Greece, pp. 1–12 (2018)
25. Ergün, N., Bülbül, K.G.: An assessment of factors affecting airport security services: an AHP approach and case in Turkey. *Secur. J.* **32**(1), 20–44 (2019)
26. Faravelli, M., Borzi, B., Pagano, M., Quaroni, D.: Using openquake to define seismic risk and real time damage scenario in Italy. In: 16th European Conference on Earthquake Engineering (2018)
27. Federal Emergency Management Agency (FEMA): NEHRP Recommended Seismic Provisions for New Buildings and Other Structures (FEMA P-2082) (2020)
28. Fema, H.: Mr3 technical manual. Multi-Hazard Loss Estimation Methodology Earthquake Model (2003)
29. Gehl, P., Cavalieri, F., Franchin, P.: Approximate bayesian network formulation for the rapid loss assessment of real-world infrastructure systems. *Reliab. Eng. Syst. Saf.* **177**, 80–93 (2018)
30. Gehl, P., Douglas, J., d' Ayala, D.: Inferring earthquake ground-motion fields with Bayesian networks. *Bull. Seismol. Soc. Am.* **107**(6), 2792–2808 (2017)
31. Gilles, S. et al.: Utilization of eler v2 and improvement of emsc earthquake impact estimation method. *NERIES JRA3-D5* (2010)
32. Goula, X., Dominique, P., Colas, B., Jara, J., Roca, A., Winter, T.: Seismic rapid response system in the eastern pyrenees. In: XIV World Conference on Earthquake Engineering, pp. 12–17 (2008)
33. Guérin-Marthe, S., Gehl, P., Negulescu, C., Auclair, S., Fayjaloun, R.: Rapid earthquake response: The state-of-the art and recommendations with a focus on european systems. *Int. J. Disaster Risk Reduct.* **52**, 101958 (2021)
34. Guidotti, R., Gardoni, P., Rosenheim, N.: Integration of physical infrastructure and social systems in communities' reliability and resilience analysis. *Reliab. Eng. Syst. Saf.* **185**, 476–492 (2019)
35. Huizer, Y., Swaan, C., Leitmeyer, K., Timen, A.: Usefulness and applicability of infectious disease control measures in air travel: a review. *Travel Med. Infect. Dis.* **13**(1), 19–30 (2015)
36. Humphries, E., Lee, S.-J.: Evaluation of pavement preservation and maintenance activities at general aviation airports in texas: practices, perceived effectiveness, costs, and planning. *Transp. Res. Rec.* **2471**(1), 48–57 (2015)
37. Jaiswal, K., Wald, D., Porter, K.: A global building inventory for earthquake loss estimation and risk management. *Earthquake Spectra* **26**(3), 731–748 (2010)
38. Julien-Laferrriere, S.: *Earthquake Qualitative Impact Assessment* (2019)
39. Kammouh, O., Gardoni, P., Cimellaro, G.P.: Probabilistic framework to evaluate the resilience of engineering systems using bayesian and dynamic bayesian networks. *Reliab. Eng. Syst. Saf.* **198**, 106813 (2020)
40. Kijko, A.: Estimation of the maximum earthquake magnitude,  $m_{max}$ . *Pure Appl. Geophys.* **161**(8), 1655–1681 (2004)
41. Kijko, A., Sellevoll, M.A.: Estimation of earthquake hazard parameters from incomplete data files. Part i. Utilization of extreme and complete catalogs with different threshold magnitudes. *Bull. Seismol. Soc. Am.* **79**(3), 645–654 (1989)

42. Kircher, C.A., Seligson, H.A., Bouabid, J., Morrow, G.C.: When the big one strikes again—estimated losses due to a repeat of the 1906 san francisco earthquake. *Earthquake Spectra* **22**(2\_suppl), 297–339 (2006)
43. Levine, N.M., Spencer, B.F.: Post-earthquake building evaluation using uavs: A bim-based digital twin framework. *Sensors* **22**(3), 873 (2022)
44. Lin, K., Wald, D., Kircher, C., Slosky, D., Jaiswal, K., Luco, N.: Usgs shakecast system advancements. In: 11th National Conference on Earthquake Engineerin, pp. 3458–3468 (2018)
45. Liu, B., Han, S., Gong, H., Zhou, Z., Zhang, D.: Disaster resilience assessment based on the spatial and temporal aggregation effects of earthquake-induced hazards. *Environ. Sci. Pollut. Res.* **27**(23), 29055–29067 (2020)
46. Maroufi, H., Borhani, M.: A measurement of community seismic resilience in sub-city districts of Mashhad, Iran. *J. Environ. Plann. Manag.* **65**(4), 675–702 (2022)
47. Midorikawa, S.: Dense strong-motion array in Yokohama, Japan, and its use for disaster management. In: *Directions in Strong Motion Instrumentation*, pp. 197–208. Springer (2005)
48. Miles, S.B., Burton, H.V., Kang, H.: Community of practice for modeling disaster recovery. *Nat. Hazards Rev.* **20**(1), 04018023 (2019)
49. Molina, S., Lang, D.H., Lindholm, C.D.: Selena—an open-source tool for seismic risk and loss assessment using a logic tree computation procedure. *Comput. Geosci.* **36**(3), 257–269 (2010)
50. Molina Hutt, C., Vahanvaty, T., Kourehpaz, P.: An analytical framework to assess earthquake-induced downtime and model recovery of buildings. *Earthquake Spectra* **38**(2), 1283–1320 (2022)
51. Motlagh, Z.S., Dehkordi, M.R., Eghbali, M., Samadian, D.: Evaluation of seismic resilience index for typical re school buildings considering carbonate corrosion effects. *Int. J. Disaster Risk Reduct.* **46**, 101511 (2020)
52. National Earthquake Hazards Reductions Program (NEHRP): *Nehrp Recommended Seismic Provisions for New Buildings and Other Structures*, vol. ii, Part 3 (2015)
53. Nuti, C., Rasulo, A., Vanzi, I.: Seismic safety of network structures and infrastructures. *Struct. Infrast. Eng.* **6**(1-2), 95–110 (2010)
54. Pasquale, G.D., Orsini, G., Romeo, R.W.: New developments in seismic risk assessment in Italy. *Bull. Earthquake Eng.* **3**(1), 101–128 (2005)
55. Poland, C.: *Defining Resilience: What San Francisco Needs from Its Seismic Mitigation Policies*. Report, San Francisco Planning and Urban Research Association (SPUR) (2009)
56. Porter, K., Jones, L., Cox, D., Goltz, J., Hudnut, K., Mileti, D., Perry, S., Ponti, D., Reichle, M., Rose, A. Z., et al.: The shakeout scenario: A hypothetical mw7. 8 earthquake on the Southern San Aandreas fault. *Earthquake Spectra* **27**(2), 239–261 (2011)
57. Rasulo, A., Pelle, A., Briseghella, B., Nuti, C.: A resilience-based model for the seismic assessment of the functionality of road networks affected by bridge damage and restoration. *Infrastructures* **6**(8), 112 (2021)
58. Sattar, S., Ryan, K., Arendt, L., Bonowitz, D., Comerio, M., Davis, C., Deierlein, G., Johnson, K.J., et al.: *Recommended Options for Improving the Built Environment for Post-Earthquake Reoccupancy and Functional Recovery Time* (2021)
59. Sedan, O., Negulescu, C., Terrier, M., Roulle, A., Winter, T., Bertil, D.: Armagedom—a tool for seismic risk assessment illustrated with applications. *J. Earthquake Eng.* **17**(2), 253–281 (2013)
60. Shimizu, Y., Yamazaki, F., Yasuda, S., Towhata, I., Suzuki, T., Isoyama, R., Ishida, E., Suetomi, I., Koganemaru, K., Nakayama, W.: Development of real-time safety control system for urban gas supply network. *J. Geotech. Geoenviron. Eng.* **132**(2), 237–249 (2006)
61. Singh, V., Sharma, S.K., Chadha, I., Singh, T.: Investigating the moderating effects of multi group on safety performance: The case of civil aviation. *Case Stud. Transp. Policy* **7**(2), 477–488 (2019)
62. Skorupski, J., Uchroński, P.: A fuzzy system to support the configuration of baggage screening devices at an airport. *Expert Syst. Appl.* **44**, 114–125 (2016)

63. Sun, L., Stojadinovic, B., Sansavini, G.: Resilience evaluation framework for integrated civil infrastructure–community systems under seismic hazard. *J. Infrastruct. Syst.* **25**(2), 04019016 (2019)
64. Sutley, E.J., van de Lindt, J.W., Peek, L.: Community-level framework for seismic resilience. i: Coupling socioeconomic characteristics and engineering building systems. *Nat. Hazards Rev.* **18**(3), 04016014 (2017)
65. Tahmasebi Birgani, Y., Yazdandoost, F.: An integrated framework to evaluate resilient-sustainable urban drainage management plans using a combined-adaptive MCDM technique. *Water Resour. Manag.* **32**(8), 2817–2835 (2018)
66. Thakur, M.: Depreciation Rate (2020). <https://www.educba.com/depreciation-rate/>
67. Tien, Y.M., Juang, C.H., Chen, J.-M., Pai, C.-H.: Isointensity-isoexposure concept for seismic vulnerability analysis—a case study of the 1999 chi-chi, Taiwan earthquake. *Eng. Geol.* **131**, 1–10 (2012)
68. Todorov, B., Billah, A.M.: Post-earthquake seismic capacity estimation of reinforced concrete bridge piers using machine learning techniques. In: *Structures*, vol. 41, pp. 1190–1206. Elsevier (2022)
69. Toma-Danila, D., Cioflan, C., Ionescu, C., Tiganescu, A.: The near real-time system for estimating the seismic damage in romania (seisdaro)—recent upgrades and results. In: *Proceedings of the 16th ECEE, Tsaloniki, Greece* (2018)
70. Trendafiloski, G., Wyss, M., Rosset, P.: Loss estimation module in the second generation software QLARM. In: *Human Casualties in Earthquakes*, pp. 95–106. Springer (2011)
71. Tsonis, G.: Seismic resilience: concept, metrics and integration with other hazards. In: *Joint Research Centre, Publications Office of the European Union, Luxembourg* (2014). <https://doi.org/10.713724>
72. US Department of Homeland Security: *National Infrastructure Protection Plan*, pp. 29–33 (2013)
73. US Nuclear Regulatory Commission: *Central and Eastern United States Seismic Source Characterization for Nuclear Facilities* (2012)
74. USC: *Seismic Standards*, author=42 U.S.C. §7705b (2018)
75. Verrucci, E., Rossetto, T., Twigg, J., Adams, B.: Multi-disciplinary indicators for evaluating the seismic resilience of urban areas. In: *Proceedings of 15th World Conference Earthquake Engineering, Lisbon* (2012)
76. Wald, D., Jaiswal, K., Marano, K., Bausch, D., Hearne, M.: *Pager–Rapid Assessment of an Earthquakes Impact*. Technical Report, US Geological Survey (2010)
77. Wald, D.J., Worden, B.C., Quitoriano, V., Pankow, K.L.: *Shakemap Manual: Technical Manual, User’s Guide, and Software Guide*. Technical Report (2005)
78. Wallace, M., Webber, L.: *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets*. Amacom (2017)
79. Wein, A., Felzer, K., Jones, J., Porter, K.: *Haywired Scenario Aftershock Sequence*, Chap. g of detweiler, st, and wein, am, eds., the *Haywired Earthquake Scenario—Earthquake Hazards*. Us Geological Survey Scientific Investigations Report 2017–5013–a–h, 126 p. (2017)
80. Willemsen, B., Cadee, M.: Extending the airport boundary: Connecting physical security and cybersecurity. *J. Airport Manag.* **12**(3), 236–247 (2018)
81. Wilson, G.: *Community Resilience and Environmental Transitions*. Routledge, Thames (2012)
82. Wilson, M., Foulger, G., Gluyas, J., Davies, R., Julian, B.: *Hiquake: The human-induced earthquake database*. *Seismol. Res. Lett.* **88**(6), 1560–1565 (2017)
83. Worden, C.B., Thompson, E.M., Baker, J.W., Bradley, B.A., Luco, N., Wald, D.J.: Spatial and spectral interpolation of ground-motion intensity measure observations. *Bull. Seismol. Soc. Am.* **108**(2), 866–875 (2018)
84. World Health Organization: *Economic Losses, Poverty & Disasters, 1998–2017* (2018)
85. Yang, C.-L., Yuan, B.J., Huang, C.-Y.: Key determinant derivations for information technology disaster recovery site selection by the multi-criterion decision making method. *Sustainability* **7**(5), 6149–6188 (2015)

86. Yeh, C.-H., Loh, C.-H., Tsai, K.-C.: Overview of taiwan earthquake loss estimation system. *Natural Hazards* **37**(1), 23–37 (2006)
87. Yin, C., Kassem, M.M., Mohamed Nazri, F., et al.: Comprehensive review of community seismic resilience: Concept, frameworks, and case studies. *Adv. Civil Eng.* **2022**, Article ID 7668214 (2022)
88. You, T., Wang, W., Chen, Y.: A framework to link community long-term resilience goals to seismic performance of individual buildings using network-based recovery modeling method. *Soil Dyn. Earthquake Eng.* **147**, 106788 (2021)
89. Yuan, X., Chen, G., Jiao, P., Li, L., Han, J., Zhang, H.: A neural network-based multivariate seismic classifier for simultaneous post-earthquake fragility estimation and damage classification. *Eng. Struct.* **255**, 113918 (2022)
90. Zhao, J.-n., Shi, L.-n., Zhang, L.: Application of improved unascertained mathematical model in security evaluation of civil airport. *Int. J. Syst. Assurance Eng. Manag.* **8**(3), 1989–2000 (2017)
91. Zhao, T., Sun, L.: Seismic resilience assessment of critical infrastructure-community systems considering looped interdependences. *Int. J. Disaster Risk Reduct.* **59**, 102246 (2021)
92. Zhou, L., Wu, X., Xu, Z., Fujita, H.: Emergency decision making for natural disasters: An overview. *Int. J. Disaster Risk Reduct.* **27**, 567–576 (2018)
93. Zülfiqar, A.C., Fercan, N. Ö. Z., Tunç, S., Erdik, M.: Real-time earthquake shake, damage, and loss mapping for istanbul metropolitan area. *Earth Planets Space* **69**(1), 1–15 (2017)

# Efficiency Evaluation of Regions' Firefighting Measures by Data Envelopment Analysis



Fuad Aleskerov and Sergey Demin

## 1 Introduction

Unfortunately, emergency situations, both natural and technological, are an integral part of the modern world. They constantly accompany people, threaten their lives, bring pain and suffering, damage and destroy material values, and cause huge, often irreparable damage to the environment, society, and civilization.

Over the past couple of decades, the number of natural disasters have increased worldwide. As a result, the number of victims and economic losses also go upward [1]. Global damage from natural disasters can amount up to about 250 billion dollars (Fig. 1). In addition, the scale of anthropogenic activities in modern society, and the complexity of technological processes increases, with the use of a significant number of explosions, fire, radiation, and chemically hazardous substances. It all emphasizes the importance of the problems associated with maintenance of security and preserving the economic potential and the environment in cases of emergency.

As we can see, globally storms are hardest problem in the world. However, in different places, climate and natural circumstances vary. And for the Russia, wildfires are one of the main problems from all possible natural disasters.

Russia is rightfully considered as a forest country, approximately 20% of all forests of the world, half of all coniferous forests are located here. Forests occupy about 50% of the total area of the Russian Federation and amount up to 1.2 billion hectares.

It is registered from 10 to 35 thousand forest fires annually on the Russian territory, covering an area of 0.5–2.5 million hectares. Taking into account the

---

F. Aleskerov · S. Demin (✉)

Department of Mathematics, Faculty of Economics, National Research University Higher School of Economics, Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia  
e-mail: [alesk@hse.ru](mailto:alesk@hse.ru); [sdemin@hse.ru](mailto:sdemin@hse.ru)

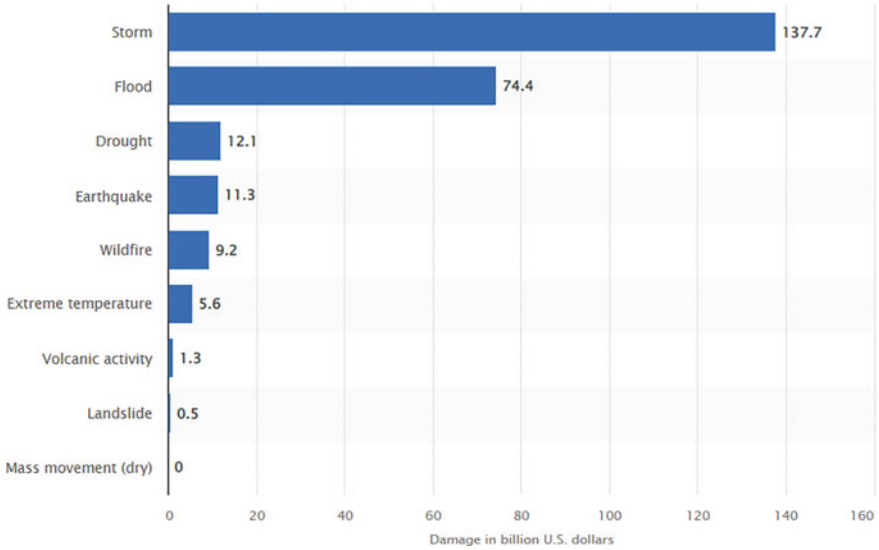


Fig. 1 Damage from different types of natural disasters in 2021

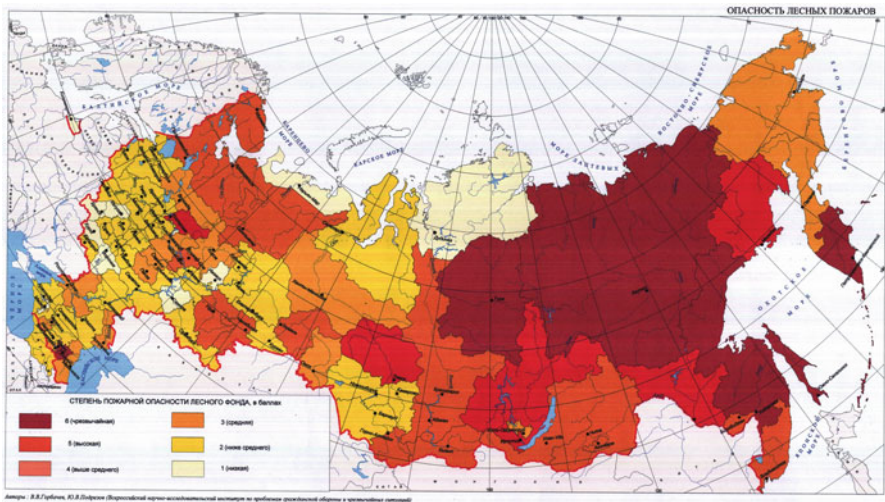


Fig. 2 Degree of fire hazard in different Russian regions

burning of a huge number of forests in the unprotected and occasionally protected territories in the northern parts of Siberia and the Far East, the total area covered by fire ranges from 2.0 to 5.5 million hectares (Fig. 2).

Wildfires cause huge damage to the environment; it takes several decades and several generations of foresters to restore the forest. In the case when industrial facilities are located in the immediate vicinity of the forest, the damage from fire



can be enormous. But the greatest danger is the threat to human settlements when a wildfire can cause the death of local people.

Since it is important to predict and mitigate the consequences of disasters, the question arises how to execute this properly in certain conditions. Given that there are still no uniform rules, the only solution seems to be just a repetition of the most successful examples. For this reason, it is crucial to determine which cases are effective and which are not.

Consequently, it is necessary to apply some methods of efficiency evaluation, compare the results for different examples, and choose the best alternative as a benchmark.

Since Huang et al. [11] claimed that quantitative assessment is very sensitive to the importance of various factors, it is decided to use linear programming approach for the efficiency assessment. Similar approach was proposed by Farrell [9] and consists of using the fraction of weighted sums of several object characteristics as its efficiency.

$$efficiency = \frac{\sum_{i=1}^M u_i y_{ik}}{\sum_{j=1}^N v_j x_{jk}}$$

Later, Charnes et al. [5] carried out new methodology based on this idea—Data Envelopment Analysis. Nowadays, it is widely used in many spheres: machine tool manufactures [6], shops [18], universities [17], public galleries [19], etc.

As mentioned above, Data Envelopment Analysis (DEA) is based on the idea of efficiency assessment of different decision-making units (DMUs) by the fraction of objects parameters. For this purpose, it is necessary to choose two groups of features which will characterize all DMUs—inputs, such as spent resources, and outputs, as obtained results [10].

In addition, considering rationality and interpretability of the results in terms of the obtained efficiency evaluations, constraints, which guarantee that the efficiency of all objects lies in the interval [0, 1] should be added.

As a result, the statement of the problem is written as

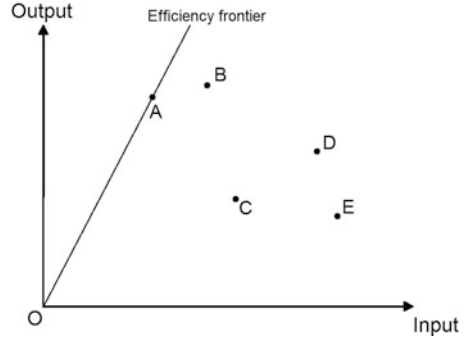
$$\max_{u_i, v_j} \frac{\sum_{i=1}^M u_i y_{ik}}{\sum_{j=1}^N v_j x_{jk}}$$

under the constraints

$$\left\{ \begin{array}{l} \forall k \frac{\sum_{i=1}^M u_i y_{ik}}{\sum_{j=1}^N v_j x_{jk}} \leq 1 \\ \forall i \ u_i \geq 0 \\ \forall j \ v_j \geq 0 \end{array} \right.$$

where  $y_{ik}$  and  $x_{jk}$  are the output and input parameters of the  $k$ -th object, while  $u_i, v_j$  are nonnegative weight coefficients, illustrating the importance of output and input features respectively.

**Fig. 3** Example of basic DEA



Solving this problem for each object in comparison, we get the optimal frontier, where the efficiency is equal to 1 (Fig. 3). For all DMUs lying below this frontier, the efficiency is evaluated using the distance from the benchmark frontier.

DEA has been applied for different disasters. For instance, Dubey et al. [8] compared 21 districts of the Narmada River basin in central India in terms of flood vulnerabilities. Aleskerov and Demin [2] analyzed technological disasters in different Russian regions. Meanwhile, Wang et al. [20] applied DEA for the efficiency evaluation of different locations for the earthquake relief warehouses.

In turn, de Almada Garcia et al. [7] proposed to use DEA for the assessment of the nuclear power plants safety. Considering complex structure of power plant, authors took into account the specification of some problems. For instance, it was claimed that the severity of the failure mode has higher level of significance than potential frequency of failures occurrence and their detectability. Therefore, it is necessary to place some constraints on the parameters weight coefficients. It allows the construction of a more realistic and more precise method, which will pay attention to the ratio of importance of different criteria.

However, for the application of the majority of DEA methods, it is necessary to get precise values of all DMU features. Meanwhile some characteristics, such as budget spendings, region area, number of employees, region number of companies, are estimated roughly, because small deviations in these characteristics are not so crucial.

Moreover, some features cannot be measured directly. For instance, in the case of a region's disaster preventive measures efficiency comparison, such features as total economic losses or the potential human losses, are evaluated using some regression models. Therefore, these parameters cannot be precise because of inaccuracy of the simulation process and are usually given as approximate values.

As a result, it is clear that in such cases it is necessary to use special modified DEA models which can work in case of lack of precise data.

One of the approaches to solve this problem is the use of fuzzy logic [13, 21]. According to this theory, the concept of a fuzzy set  $A = \{(x, \mu_A(x)) | x \in X\}$ , where  $\mu_A(x)$  is the membership function (a generalization of the concept of a characteristic function for ordinary clear sets), which indicates the measure of membership of element  $x$  to set  $A$ . By replacing the unambiguous exact values of the parameters

of the objects being compared with similar fuzzy sets, the membership function corresponding to set  $A$  acquires the meaning of the probability of equality of the true value of the parameter to a specific number.

Thus, it was proposed to apply  $\alpha$ -slices ( $A_\alpha = \{x \in X | \mu_A(x) \geq \alpha\}$ ) and the extension principle to transform the basic model of data envelopment analysis [12]. The upper and lower bounds of the membership functions for evaluating efficiency are determined at a fixed level  $\alpha$ .

Afterwards it was proposed to use certain types of fuzzy sets. At first, triangular fuzzy numbers have been considered [14]:

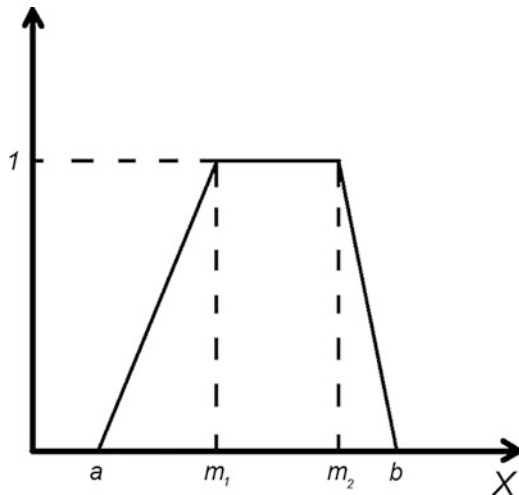
$$\mu_A(x) = \begin{cases} \frac{x-a}{m-a}, & a \leq x \leq m, \\ \frac{b-x}{b-m}, & m \leq x \leq b, \\ 0, & \text{otherwise.} \end{cases}$$

It was proposed to replace all input and output parameters with such triangular numbers in the optimization problem of weight coefficients calculation. At the same time, the weights themselves remain ordinary real numbers.

A slightly more general variant of fuzzy sets used in shell data analysis are trapezoidal fuzzy numbers ([15], Fig. 4):

$$\mu_A(x) = \begin{cases} \frac{x-a}{m_1-a}, & a \leq x \leq m_1, \\ 1, & m_1 \leq x \leq m_2, \\ \frac{b-x}{b-m_2}, & m_2 \leq x \leq b, \\ 0, & \text{otherwise.} \end{cases}$$

**Fig. 4** Trapezoidal fuzzy number



## 2 Framework

Below, we apply interval modification of DEA methods which helps to solve the highlighted problem. We discard all aforementioned stochastic and probabilistic approaches based on fuzzy logic [4, 16]. Indeed, in some cases it might be too demanding to request stochastic or probabilistic evaluations of parameters. That is why we use simple intervals for the parameter assessment instead of single value (pair  $(y_{ik}^-, y_{ik}^+)$  instead of  $y_{ik}$ ). In addition, we use for the comparison of the objects specified methodology for the parameters' value comparison ( $>_i$ —comparison according to the  $i$ -th output feature):

$$object_k >_i object_l \iff y_{ik}^- > y_{il}^+$$

In turn, if intervals  $(y_{ik}^-, y_{ik}^+)$  and  $(y_{il}^-, y_{il}^+)$  are intersecting (both inequalities  $y_{ik}^+ > y_{il}^-$  and  $y_{il}^+ > y_{ik}^-$  hold), objects  $k$  and  $l$  are incomparable. For instance, in Fig. 5, there are three objects, and two pairs ( $l$  and  $k$ ,  $k$  and  $m$ ) are incomparable. In turn, objects  $l$  and  $m$  can be compared according to  $y_i$  interval of  $m$  is completely higher than interval of  $l$ , therefore  $m >_i l$ .

Using this type of data representation and parameters comparison, we can apply modified “best tube” IDEA.

The core idea of this approach is based on the idea that some DMUs might be near the efficiency frontier [3]. But, in the case of classic version of DEA, they will not get 100% efficiency. According to the “best tube” IDEA, we assign 100% efficiency, not only to the objects on the best efficiency frontier, but also to the DMUs, which are incomparable with them. Meanwhile, efficiency of all other DMUs is evaluated by the basic DEA.

However, this method does not pay attention to the objects which might be near the efficiency frontier, but far from optimal DMUs (for example, object F in Fig. 6).

Therefore, in this work we propose to modify procedure of choosing “almost best” objects. For this purpose, instead of the finding DMUs, which are incomparable with 100% objects, we choose all objects, whose optimal version (minimal input and maximum output parameters) lies above efficiency frontier.

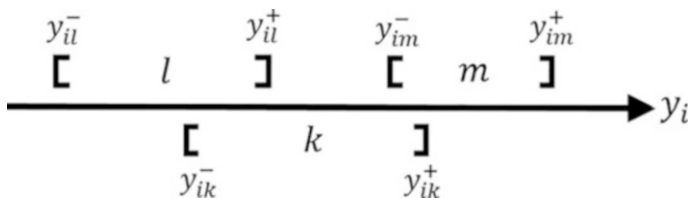
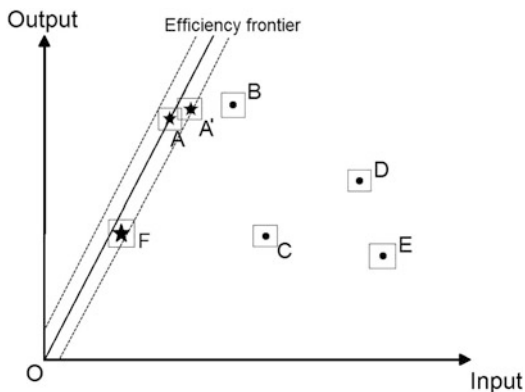


Fig. 5 Comparison of interval feature values

**Fig. 6** An example of “best tube” IDEA application



### 3 Application of the Model

We compare firefighting policies in different Russian regions. For proper efficiency analysis, it is important to choose wisely DMUs objects, which will be taken into account.

Achieved results of preventive firefighting measures are surely connected with happened wildfires. However, it is important to consider not only the number of disasters, but also their “quality.”

Sometimes damage of different disasters is measured in economic losses or the number of injured and dead, however here it will be hard to evaluate even approximate data, because of huge territories. Therefore, instead of these parameters we consider total area covered with wildfires. Certainly, this approach has one disadvantage because some regions have an opportunity to control these outputs by choosing better moment of data collection and choose to claim several small wildfires or wait some time and afterwards claim only one united wildfire with higher total area. We try to overcome this problem with data collection for the whole year, so regions will collect the data only after the occurred disaster. In addition, in order to consider the size of the region output parameters are divided by the total area of the regions.

In turn, it will be great to use as input parameters the total budget spendings on firefighting measures. However, unfortunately these data are not available. So, we choose to use the closest budget categories—investments in agriculture and forestry and expenditures on environmental protection.

In addition, it is important to choose the set of compared regions so that all analyzed DMUs should face with the problem of wildfires. Because otherwise some districts will put too high benchmark and the majority of regions will obtain too low and indistinguishable efficiency evaluations. For this purpose, we analyzed only 46 regions of the Russian Federation with at least ten wildfires.

## 4 Results and Analysis

Applying different methodologies, we got two efficiency evaluations for each region. On this basis, we construct rankings of the Russian regions, according to each of approaches.

As expected, both methods give us similar results with minor distinguishes (the best regions are presented in Table 1 and the worst regions—in Table 2). The main difference is that best tube DEA evaluates milder and gives higher efficiency assessments, because it assigns 100% result to some additional objects in the comparison set, which obtain lower values according to basic DEA. In addition, the benchmark for all inefficient DMUs goes lower and improves their efficiency.

Analyzing obtained rankings, it is necessary to examine the best and the worst objects from the set. Speaking of leaders, Tambov and Samara Oblasts are small regions, while mountainous terrain prevails in Chukotka, and only in the coastal part, as well as along the river valleys, there are small territories occupied by lowlands and forests. Therefore, it is fairly easy for these regions to cope with wildfires on their territory.

**Table 1** Regions with the best wildfire preventive measures

	Basic DEA	Best tube IDEA
Tambov Oblast	1	1
Samara Oblast	1	1
Chukotka Autonomous District	1	1
Kaluga Oblast	0.93	1
Sakhalin Oblast	0.88	1
Republic of Karelia	0.87	1
Republic of Khakassia	0.79	0.97
Ulyanovsk Oblast	0.72	0.85
Penza Oblast	0.63	0.77
Yamalo-Nenets Autonomous District	0.56	0.69

**Table 2** Regions with the worst wildfire preventive measures

	Basic DEA	Best tube IDEA
Krasnoyarsk Krai	0.002	0.002
Republic of Sakha (Yakutia)	0.003	0.004
Irkutsk Oblast	0.005	0.006
Sverdlovsk Oblast	0.012	0.014
Chelyabinsk Oblast	0.016	0.019
Omsk Oblast	0.023	0.028
Khabarovsk Territory	0.028	0.034
Republic of Bashkortostan	0.032	0.037
Maritime Territory	0.033	0.040
Transbaikal	0.033	0.040

Meanwhile the worst regions, Krasnoyarsk Krai, Republic of Sakha (Yakutia), Irkutsk Oblast, and Sverdlovsk Oblast, obtain very low efficiency assessment—lower than 2%.

It might be mentioned in their defense that all these regions have huge territories and low population density. For instance, Republic of Sakha is the world's largest country subdivision (over three million square kilometers) with only 0.32 human being per km<sup>2</sup>. It is clear that, under such circumstances it is really hard to efficiently fight with wildfires, especially considering that 80% of the region territory is covered with forests.

## 5 Conclusion

We applied modified interval DEA model to different regions of the Russian Federation. It helped to find out that considering some uncertainties in the data efficiency in some regions is higher than according to the basic DEA. Meanwhile, obtained rankings of regions are similar so the list of leaders and outsiders stay the same, which shows that the main practical difference in these methods is the strictness of the model. We truly believe that using best tube DEA might help in many similar cases with approximate features values.

**Acknowledgments** This work is an output of a research project implemented as part of the Basic Research Program at the National Research University Higher School of Economics (HSE University).

## References

1. Ahmad, J., Sadia, H.: Natural disasters assessment, risk management, and global health impact. In: *Handbook of Global Health*. Springer (2020)
2. Aleskerov, F., Demin, S.: An assessment of the impact of natural and technological disasters using a DEA approach. In: *Dynamics of Disasters—Key Concepts, Models, Algorithms, and Insights*, pp. 1–14. Springer (2016)
3. Aleskerov, F.T., Demin, S.: Chapter 2: DEA for the assessment of Regions' ability to cope with disasters, dynamics of disasters. In: *Impact, Risk, Resilience, and Solutions*, pp. 31–37 (2021)
4. Bagheri, M., Ebrahimnejad, A., Razavyan, S., Lotfi, F.H., Malekmohammadi, N.: Solving fuzzy multi-objective shortest path problem based on data envelopment analysis approach. *Complex Intell. Syst.* **7**(4), 725 (2021)
5. Charnes, A., Cooper, W.W., Rhodes, E.: Measuring the efficiency of decision making units. *Eur. J. Oper. Res.* **2**, 429–444 (1978)
6. Chen, J.-L.: Business efficiency evaluation of machine tool manufacturers by data envelopment analysis (DEA): a case study of Taiwanese listed machine tool companies. *Int. Bus. Res.* **14**(12), 125–134 (2021)
7. De Almada Garcia Adriano, P., Curty Leal Junior, I., Alvarenga Oliveira, M.: A weight restricted DEA model for FMEA risk prioritization. *Producao.* **23**(3), 500–507 (2013)

8. Dubey, S., Kulshrestha, M., Kulshrestha, M.: Flood vulnerability assessment using data envelopment analysis – the case of Narmada river basin districts in Central India. *Water Policy*. **23**(9), 1089 (2021)
9. Farrell, M.J.: The measurement of productive efficiency. *J. R. Stat. Soc. Ser. A (General)*. **120**(3), 253–290 (1957)
10. Golany, B., Roll, Y.: An application procedure for DEA. *Omega*. **17**(3), 237–250 (1989)
11. Huang, J., Liu, Y., Ma, L.: Assessment of regional vulnerability to natural hazards in China using a DEA model. *Int. J. Disaster Risk Sci.* **2**(2), 41–48 (2011)
12. Kao, C., Liu, S.T.: Fuzzy efficiency measures in data envelopment analysis. *Fuzzy Sets Syst.* **113**(3), 427–437 (2000)
13. Klaua, D.: An early approach toward graded identity and graded membership in set theory. *Fuzzy Sets Syst.* **161**(18), 2369–2379 (1965)
14. Kuamr, N., Singh, A.: Efficiency evaluation of select Indian banks using fuzzy extended data envelopment analysis. *Int. J. Inf. Decis. Sci.* **9**(4), 334–352 (2017)
15. Lertworasirikul, S., Fang, S.-C., Joines, J.A., Nuttle, H.L.W.: Fuzzy data envelopment analysis (DEA): a possibility approach. *Fuzzy Sets Syst.* **139**(2), 379–394 (2003)
16. Namakin, A., Najafi, S.E., Fallh, M., Javadi, M.: A new evaluation for solving the fully fuzzy data envelopment analysis with Z-numbers. *Symmetry*. **10**, 384 (2018)
17. Saljooghi, F.H., Rayeni, M.M.: Network data envelopment analysis model for estimating efficiency and productivity in universities. *J. Comput. Sci.* **6**(11), 1252–1257 (2010)
18. Segota, A.: Evaluating shops efficiency using data envelopment analysis: categorical approach. *Proc. Rijeka School Econ.* **26**(2), 325–343 (2008)
19. Vrabková, I., Bečica, J.: The technical and allocative efficiency of the regional public galleries in The Czech Republic. *SAGE Open*. **11**(2), 1–15 (2021)
20. Wang, Y., Xu, G., Zhang, W., Zhou, Z.: Location analysis of earthquake relief warehouses: evaluating the efficiency of location combinations by DEA. *Emerg. Mark. Financ. Trade*. **56**(8), 1752–1764 (2020)
21. Zadeh, L.A.: Fuzzy sets. *Inf. Control*. **8**(3), 338–353 (1965)



# Superposition Principle for Tornado Prediction



Fuad Aleskerov, Sergey Demin, Sergey Shvydun, Theodore Trafalis, Michael Richman, and Vyacheslav Yakuba

## 1 Introduction

Tornadoes are a major disaster hazard. For instance, direct losses to the US economy, caused by tornadoes for the period from 2010 to 2014 were about 16.5 billion dollars (NOAA, US National Weather Service). Therefore, accurately forecasting these events, as far in advance as possible (long lead time), is an important research activity.

However, achieving forecasts with long lead times is difficult because tornadogenesis process is still not completely understood and the time scale of some of the forcing mechanisms is on the order of minutes [13, 22]. Further, it has been noted that a crucial part of the space-scale process is on the order of centimeters (microscale), therefore, chaotic, which makes prediction of tornado even more complicated [12, 16].

The approach to model tornadogenesis using dynamic processes is time and resource consuming, and owing to the small spatial scale of a tornado relative to the resolution of most numerical models, physically based numerical weather prediction models still do not provide very good results [1, 9, 11]. Until measurement systems can account for every centimeter of the atmosphere and computational resources improve commensurately, allowing for the set of nonlinear equations that describe the atmosphere to be modeled, dynamic improvements will be a slow process. Until that time, there is an opportunity for data-driven methods to help improve the accuracy and lead time of existing forecasts.

---

F. Aleskerov (✉) · S. Demin · S. Shvydun · V. Yakuba  
Institute of Control Sciences of Russian Academy of Sciences, HSE University, Moscow, Russia  
T. Trafalis · M. Richman  
University of Oklahoma, Norman, OK, USA

In this work, we propose a new approach into disaster prediction by using the methods of smart data analysis for detecting tornadic circulations from the set of all observations. As a result, constructed models predict tornado occurrence with higher efficiency. In addition, smart data analysis methods work faster than simulation by dynamic weather prediction models, allowing extra time for reacting and preventing dangerous repercussions of the disaster.

The basic goal here is to find the main patterns between different characteristics of air circulation and, given these patterns, detect tornadoes. For this purpose, the following parameters of air circulations are used—temperature, air pressure, relative humidity, velocity of the air flow, and many other physical characteristics of the near-storm atmosphere.

There are numerous procedures that allow choosing alternatives from the initial set. In this work, we consider choice procedures of a special type based on the superposition principle [3, 5].

Superposition has several advantages. First, the computational complexity of the model can be managed. Unfortunately, most existing machine learning algorithms have a high computational complexity, so they cannot be applied in the case of a large number of observations or/and criteria. The use of superposition model allows reducing the complexity by applying methods with a low computational complexity on first stages and more accurate methods on final stages. Consequently, our models can be applied to larger initial datasets.

Second, superposition allows us to combine different methods and use several criteria simultaneously on each step. Moreover, models based on the idea of superposition can be interpreted easily since we can apply several simple methods instead of a complicated one. In addition, superposition will help to reduce the influence of drawbacks of initial methods. Hence, our model may have advantages of all previous techniques.

## 2 Literature Review

We consider here only the studies on application of smart data analysis methods to the tornado prediction.

Adrianto et al. [2] proposed the use of support vector machines (SVM) for tornado prediction, i.e., the algorithm constructs a hyperplane that separates a set of elements into two classes (e.g., tornadoes and non-tornadoes).

The defining function is presented as a dot product of two vectors. The first one is a vector of circulation attributes, such as wind speed, temperature, air pressure on the surface, relative humidity at different levels, etc. In turn, the second vector consists of weight coefficients, which show the importance of each parameter in tornado prediction process. Therefore, a small absolute value of the weight coefficient for a particular parameter means that the parameter can hardly influence future tornado detection. Correspondingly, high value of the coefficient indicates high prediction power of the attribute.

However, given the nonlinear relationships that lead to tornadogenesis, the accuracy of all methods based on linear regression is low. Recently, Trafalis et al. [24] also proposed other approaches to this problem.

The first mentioned technique is an improvement of the aforementioned method of support vector machines with reverse features elimination (SVM-RFE). According to this approach, one should implement the standard SVM algorithm and compute the weight coefficients. Afterwards the attribute which has the lowest value of the weight coefficient is eliminated from the features list. Subsequently, the algorithm iteratively continues until only one parameter remains.

At the end of the process, the sequence of eliminated attributes is transformed into the ranking of the parameters by using the rule that the number of the attributes in the ranking are equal to the number of iterations (backward), when the attribute was eliminated.

However, the ranking is not the only goal of this method. Some features of atmospheric circulation might be prone to giving false alarms with tornado detection; therefore, the last step of the SVM-RFE algorithm is the choice of the number of parameters which are used for tornado detection. For this purpose, one evaluates the accuracy of the method according to the number of used attributes (it is important to point out that the algorithm uses only top attributes from the ranking).

One more method proposed for tornado prediction is a neural network approach [10, 14, 15]. The main idea is the construction of a nonlinear function that maps real-valued input variables to a number varying between 0 and 1. The most popular version of neural network is used (a three-layer perceptron network). Such a neural network has one hidden layer of neurons.

The next proposed technique is Random Forest method (RANF), developed by Breiman [7]. It is a group classifier with multiple decision trees, wherein each tree is trained on a part of all attributes, chosen randomly. Consequently, the predictions of all trees are aggregated by the classification based on the majority rule of the votes over all classifiers.

The last proposed algorithm is Rotation Forest method (ROTF) by Rodriguez et al. [18]. This method utilizes principal component analysis (PCA) to distinguish attributes which are used to construct a decision forest. This forest consists of decision trees which are trained on the whole data set in a rotated feature space. The set of parameters are randomly divided into  $K$  groups. Afterwards, principal component analysis is performed simultaneously on each group. As a result, we receive  $K$  classifiers that compose one classification instrument. This instrument works in the same way as RANF; classification is based on the majority of the votes over all trees.

It is important to note that each of the aforementioned methods has specific drawbacks, which decrease the accuracy of tornado prediction, namely, all techniques detect only a fraction of the tornadoes (more than 25% of all tornadoes are missed). In addition, a significant part of tornado signals (about 20%) is false alarm, which is also very important. Thus, general accuracy of these methods (from 51% to 57%) is sufficient for operational application.

In this work, we use choice functions, based on the superposition principle [3, 5] to make tornado prediction. Usually, a standard choice function  $C(\bullet)$  consists in the choice of some subset of alternatives that satisfy a predefined condition.

Ideally the specified condition should be “being tornadic circulation.” However, in real life, it is difficult to satisfy this condition. Hence, we use some simpler conditions, which narrow the initial set of observations and get trustworthy results by application of the superposition principle.

Superposition of two choice functions  $C_1(\bullet)$  and  $C_2(\bullet)$  is a binary operation  $\odot$ , the result of which is a new function  $C^*(\bullet) = C_2(\bullet) \odot C_1(\bullet)$ , which has a form  $\forall X \in 2^A C^*(X) = C_2(C_1(X))$ ,  $A$  being the set of all observations [3]. In short, the latter function  $C_2(\bullet)$  is used on the data obtained by the application of the former one  $C_1(\bullet)$ . It is necessary to mention that in the case of change of methods’ application order, the result might be totally different, as the superposition is not commutative operation and the functions  $C_1(\bullet)$  and  $C_2(\bullet)$  can be completely diverse. The properties of the superposition operator were studied in [3, 4, 20, 21] and other papers.

### 3 Preliminary Data Analysis

#### 3.1 Data Description

Here we use the same data as Richman et al. [17]. It is the dataset of meteorological parameters, circulations, and observations calculated by application of the National Severe Storms Laboratory Mesocyclone Detection Algorithm (MDA) [23] and near-storm environment (NSE) algorithm from Doppler radar velocity data. These two methods were developed at the National Severe Storms Laboratory [8]. The main idea of these methods is an analysis of azimuthal shear in Doppler radar velocity and rotational strength data in three dimensions.

In this dataset we have 10,816 observed circulations (721 of them are tornadic circulations) taken from 111 storm days. Unfortunately, these storm days are not consecutive—these circulations took place in the time period from 1995 to 1999. All observations contain 83 attributes (Table in the Appendix), which describe physical characteristics (e.g., pressure, temperature, wind velocity). In addition, one parameter shows the date of circulation occurrence (month). In turn, the target parameter is binary (tornado or non-tornado), which means that our problem is classification of these data into two classes.

Additionally, it is important to highlight some specific features of these data which complicate their use for tornado prediction. For instance, in some cases, multiple observations account for one air circulation. The difference between them is explained by the fact that one mesocyclone was detected at different times by different radars.

Since there is an assumption that the parameters leading to tornadogenesis are location invariant, the dataset does not contain an information about the place, where observation was made. Thus, we have neither information about any characteristics of observation location (terrain details or distance from the ocean, for instance), nor even approximate location (for example, state).

Any data mining process requires data preprocessing, such as deleting duplicate or outlying values and verification of value intervals. In addition, in some situations, it can be important to check measure units. Detailed description of these procedures applied to the data under study can be found in Aleskerov et al. [6].

### ***3.2 A Correlation of the Parameters***

To decrease the amount of information analyzed, we have examined the data more thoroughly and chosen parameters which are more important in our model.

For this purpose, we examined the Pearson correlation between different parameters to detect attributes with high correlation. These characteristics can be discarded, because we can predict the value of one parameter using the value of the other one [6].

### ***3.3 An Analysis of the Distribution of Parameters***

The next step of choosing characteristics consists of selecting parameters that have different distribution of the tornadic and non-tornadic circulations. This procedure helps us to detect tornadoes in the following way. If a parameter has different distribution for circulations of different types, it has ranges, where tornadic circulations occur more rarely. As a result, we can be more confident that certain circulation is non-tornadic.

For instance, on Fig. 1 we can see the distribution of tornadic and non-tornadic circulations according to the parameter V3 (meso depth of the circulation). For this parameter, if an element has a small value in the range 0–1,000 m, we can claim that it does not seem to be a tornado. In other words, it remained a mesocyclone that did not reach the ground. Meanwhile, if the value is in the range 10,000–12,000 m, the mesocyclone has a higher possibility to become a tornado.

### ***3.4 Additional Considerations***

The next step will help us to add attributes of circulation, which have not been highlighted. We divided the list of all parameters into two parts: a priori characteristics, which give a signal for tornado occurrence beforehand, and a posteriori ones, which

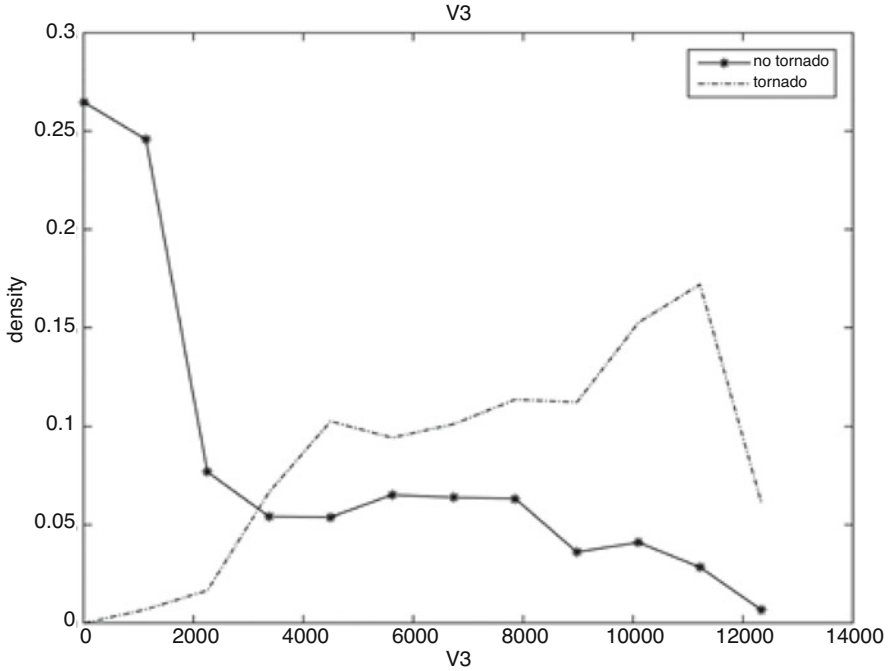


Fig. 1 Distribution of tornadic and non-tornadic circulation according to V3 (meso depth)

only fix the prediction when the disaster has already happened. For instance, such attribute as meso low-level rotational velocity might be good a priori predictor of tornadogenesis. However, in these data, we did not find evidence that this is the case and excluded it. Afterwards choosing only a priori parameters gives us the final list of characteristics used in finding patterns.

### 4 Framework

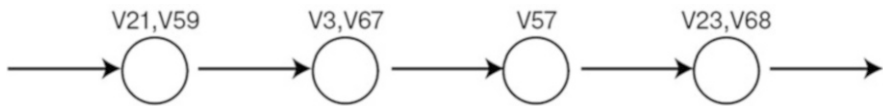
Consider a finite set  $A$  of alternatives evaluated by  $n$  parameters, i.e., the vector of values  $(u_1(x), \dots, u_n(x))$  is assigned to each alternative  $x$  from  $A$ , i.e.,  $x \in A \rightarrow (u_1(x), \dots, u_n(x))$ .

The problem lies in constructing a transformation  $C(\bullet)$ —the rule of aggregation over  $A$ —such that  $C(\bullet) : A \rightarrow R^1$ .

Our model is based on a superposition principle, applied for different choice functions. There are different ways on how to construct a choice function  $C(\bullet)$ . One of the options is provided below:

**Table 1** Parameters used for construction of an example of choice functions' composition

Attribute number	Meaning of the attribute
V3	Meso depth (m) [0–13,000]
V21	Meso strength index (MSI) “rank” [0–25]
V23	Meso low-level convergence (m/s) [0–70]
V57	Average parcel LCL (m agl)
V59	Average RH (percent) below the average parcel’s LCL
V67	0–1 km sheer magnitude (knots)
V68	0–3 km sheer magnitude (knots)



**Fig. 2** Example of choice functions' superposition (inscriptions above the vertices present the parameters used at this stage)

$$\forall X \subseteq A \quad C(X) = \{y \in X \mid \alpha_i u_i(y) + \alpha_j u_j(y) \geq b\},$$

where  $u_i(\bullet)$  and  $u_j(\bullet)$  are the values of two exact parameters  $i, j \in \{1, \dots, n\}$  of an observation, while  $b$  is the threshold value that depends on the initial set  $X$  and chosen parameters  $i$  and  $j$ . In turn, the values  $\alpha_i, \alpha_j$  are automatically defined by the following least-squares problem:

$$\left\{ \begin{array}{l} \min_{\alpha_i, \alpha_j} \sum_{l=1}^N e_l \\ e_l = (t_l - \hat{t}_l)^2 \forall l = 1, \dots, N \\ \hat{t}_l = \alpha_i u_i(y_l) + \alpha_j u_j(y_l) \forall l = 1, \dots, N, \end{array} \right.$$

where  $t_l$  is the variable, which shows the binary value of  $l$ -th observation (tornado or no tornado);  $N$  is the number of observations in the dataset  $X$ .

Note that other forms of the choice function can be used in the model.

As a result, we obtain subgroups of tornadic observations and work with them sequentially. For example, in case of using parameters from Table 1, we got the following composition of choice functions (Fig. 2). On this figure, parameters which were used for alternatives selection are written above the vertices.

The main idea of our model is the construction of a certain number of such superposition sequences in order to distinct tornadic and non-tornadic observations. Afterwards, we combine them, and the resulting prediction of our model will be the union of observation sets, obtained by different superpositions.

## 5 Application of the Model

As it was mentioned above, we apply our model to the preprocessed data obtained from the University of Oklahoma. For the correct application, we need to construct training and testing datasets, so we divided our dataset into two parts in the ratio 70:30, where the larger part is the training set.

However, here we face the following problem. At the end of the study, we will compare our model with the previous ones. In their study, Trafalis et al. [24] used another separation ratio—they divided the original dataset into two equal parts. As a result, if we use the standard ratio, the comparison would not be correct, because increasing the size of training dataset improves the accuracy of the model. Thus, we decided to apply the model twice. The first application will use equal separation and help us to compare the results. In turn, the second application will use standard data division ratio and show the accuracy of the model in standard conditions.

After the data sampling, it is important to choose the metrics for model comparison/evaluation, because there are numerous available “efficiency calculations.” In Table 2, four of them are presented.

Analyzing the efficiency calculation methods, at the first stage we reject Probability of Detection and False Alarm Ratio, because any one of these techniques does not take into account a significant part of the results. For instance, the former takes into consideration only predictions for tornadic circulations. In turn, the latter does not consider the number of missed tornadoes. Two methods would need to be examined in tandem to obtain a characterization of the model.

At the second stage we should choose between Classification Accuracy (CA) and Critical Success Index (CSI). Given the imbalance of the data, wherein about 93% of observations are non-tornadic, we reject Classification Accuracy since if we use Classification Accuracy, all models will have almost the same results. Thus, we choose Critical Success Index as the arbiter of success.

When all preparations are over, we apply the constructed tornado prediction model and evaluate its efficiency. As a result, we obtained the following results (Table 3) for 50:50 division ratio (the tornado prediction procedure was repeated 20 times and the value in Table 3 is the mean value—the efficiency is equal to 0.61).

In turn, in case of standard 70:30 data division for training and testing sets, the efficiency of our model is even higher and equal to 0.63.

**Table 2** Different efficiency calculation methods

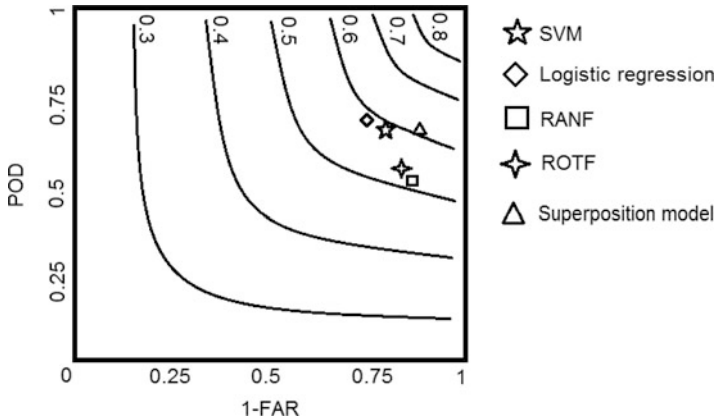
Efficiency calculation method	Formula
Classification accuracy	$CA = \frac{tp+tn}{tp+tn+fp+fn}$
Probability of detection	$POD = \frac{tp}{tp+fn}$
False alarm ratio	$FAR = \frac{fp}{tp+fp}$
Critical success index	$CSI = \frac{tp}{tp+fp+fn}$

*tp*, true positive prediction; *fp*, false positive prediction; *tn*, true negative prediction; *fn*, false negative prediction



**Table 3** Comparison of the constructed model with previous works

Prediction technique	POD	FAR	CSI
SVM	0.68	0.22	0.57
Logistic regression	0.7	0.25	0.57
RANF	0.58	0.17	0.51
ROTF	0.61	0.21	0.53
Superposition with mixed parameters	0.68	0.16	0.61



**Fig. 3** Roebber’s performance diagram for the performance results of all classifiers. The solid lines represent CSI

Comparing all tornado prediction methods in terms of three techniques of efficiency evaluation (POD, FAR, and CSI), we will get the following Roebber’s [19] performance diagram (Fig. 3).

As we can see, the improved decision tree Pareto-dominates all other models except slight predominance of logistic regression in terms of probability of detection.

## 6 Conclusion

As it was expected, the results of the improved decision tree model exceed the results of all models, which were applied before. The improvement arises as the false alarm ratio is notably smaller with this technique. There is a small tradeoff of POD, compared to logistic regression. According to meteorologists’ opinion, a skill improvement equal to 0.05 is significant development [24]. As CSI is an important component of skill, the constructed model is a successful attempt to improve the tornado prediction technique. Therefore, the improved decision tree model provides the best opportunity to obtain accurate tornado formation predictions with sufficient lead times.

**Acknowledgments** For colleagues from the HSE University, this work is an output of a research project implemented as part of the Basic Research Program at the National Research University Higher School of Economics (HSE University).

## References

1. Adlerman, E.J., Droegemeier, K.K., Davies-Jones, R.: A numerical simulation of cyclic mesocyclogenesis. *J. Atmos. Sci.* **56**, 2045–2069 (1999)
2. Adrianto, I., Trafalis, T.B., Lakshmanan, V.: Support vector machines for spatiotemporal tornado prediction. *Int. J. Gen. Syst.* **38**(7), 759–776 (2009)
3. Aizerman, M., Aleskerov, F.: *Theory of Choice*. Elsevier, North-Holland (1995)
4. Aleskerov, F., Cinar, Y.: ‘q-Pareto-scalar’ two-stage extremization model and its reducibility to one-stage model. *Theor. Decis.* **65**, 291–304 (2008)
5. Aleskerov, F., Mitichkin, E., Chistyakov, V., Shvydun, S., Iakuba, V.: Method for Selecting Valid Variants in Search and Recommendation Systems (Variants) Patent Scope, Certificate, Publication Number US10275418B2, International Application Number WO2014148948A1, Publication Date 30.04.2019. World Intellectual Property Organization (2014)
6. Aleskerov, F.T., Baiborodov, N., Demin, S.S., Richman, M., Shvydun, S.V., Trafalis, T., Yakuba, V.I.: Constructing an Efficient Machine Learning Model for Tornado Prediction, 24 p. Higher School of Economics Publishing House, Moscow (2016). WP7/2016/05
7. Breiman, L.: Random forests. *Mach. Learn.* **45**(1), 5–32 (2001)
8. Kingfield, D.M., LaDue, J.G., Ortega, K.L.: An evaluation of tornado intensity using velocity and strength attributes from the WSR-88D mesocyclone detection algorithm. In: 26th Conference on Severe Local Storms, American Meteorological Society, 3.2 (2012). Preprints
9. Kosiba, K., Wurman, J.: The three-dimensional axisymmetric wind field structure of the Spencer, South Dakota (1998) tornado. *J. Atmos. Sci.* **67**, 3074–3083 (2010)
10. Lakshmanan, V., Stumpf, G., Witt, A.: A neural network for detecting and diagnosing tornadic circulations using the mesocyclone detection and near storm environment algorithms. In: *21st International Conference on Information Processing Systems, San Diego, CA, American Meteorological Society* (2005), CD-ROM J5.2
11. Lee, B.D., Wilhelmson, R.B.: The numerical simulation of non-supercell Tornadogenesis. Part I: initiation and evolution of Pretornadic mesocyclone circulations along a dry outflow boundary. *J. Atmos. Sci.* **54**, 32–60 (1996)
12. Lewellen, D.C., Gong, B., Lewellen, W.S.: Effects of fine-scale debris on near-surface tornado dynamics. *J. Atmos. Sci.* **65**, 3247–3262 (2007)
13. Markowski, P.M., Richardson, Y.P.: Tornadogenesis: our current understanding, forecasting considerations, and questions to guide future research. *Atmos. Res.* **93**, 3–10 (2009)
14. Marzban, C.: A neural network for tornado diagnosis. *Neural Comput. & Applic.* **9**, 133–141 (2000)
15. Marzban, C., Stumpf, G.: A neural network for tornado prediction. *J. Appl. Meteorol.* **35**, 617 (1996)
16. Rhodes, C.L., Senkbeil, J.C.: Factors contributing to tornadogenesis in landfalling Gulf of Mexico tropical cyclones. *Meteorol. Appl.* **21**, 940–947 (2014)
17. Richman, M.B., Trafalis, T.B., Adrianto, I.: Chapter 4: Missing data imputation through machine learning algorithms. In: Haupt, et al. (eds.) *Artificial Intelligence Methods in the Environmental Sciences*, pp. 153–169. Springer (2008)
18. Rodriguez, J.J., Kuncheva, L.I., Alonso, C.J.: Rotation Forest: a new classifier ensemble method. *IEEE Trans. Pattern Anal. Mach. Intell.* **28**(10), 1619–1630 (2006)
19. Roebber, P.J.: Visualizing multiple measures of forecast quality. *Weather Forecast.* **24**, 601–608 (2009)

20. Shvydun, S.: Normative Properties of Multi-Criteria Choice Procedures and their Superpositions: I Working paper WP7/2015/07 (Part 1), 74 p. Higher School of Economics Publishing House, Moscow (2015a)
21. Shvydun, S.: Normative Properties of Multi-Criteria Choice Procedures and their Superpositions: II Working paper WP7/2015/07 (Part 2), 55 p. Higher School of Economics Publishing House, Moscow (2015b)
22. Straka, J.M., Rasmussen, E.N., Davies-Jones, R.P., Markowski, P.M.: An observational and idealized numerical examination of low-level counterrotating vortices toward the rear flank of supercells. *Electron. J. Severe Storms Meteorol.* **2**(8), 1–22 (2007)
23. Stumpf, G.J., Witt, A., Mitchell, E.D., Spencer, P.L., Johnson, J.T., Eilts, M.D., Thomas, K.W., Burgess, D.W.: The National Severe Storms Laboratory mesoscale detection algorithm for WSR-88D. *Weather Forecast.* **13**, 304–326 (1998)
24. Trafalis, T.B., Adrianto, I., Richman, M.B., Lakshmiarahan, S.: Machine-learning classifiers for imbalanced tornado data. *Comput. Manag. Sci.* **11**, 403–418 (2014)

# A Network-Based Risk-Averse Approach to Optimizing the Security of a Nuclear Facility



Eugene Lykhovyd, Sergiy Butenko, Craig Marianno, and Justin Yates

## 1 Introduction

Nuclear security is among the most critical issues in global policymaking [12]. The physical security of nuclear facilities is of particular importance nowadays due to the ever-increasing level of threats associated with terrorism and tensions in international relations. Hence, this topic has been attracting a significant amount of research effort in academia and governmental laboratories in the last several decades, yielding general guidelines and recommendations concerning various aspects of nuclear security [4, 8, 9].

The Design and Evaluation Process Outline (DEPO) framework is commonly used to analyze and enhance the physical security of nuclear facilities [8]. In particular, Estimation of Adversary Sequence Interruption (EASI) model is typically utilized for estimation of outcomes resulting from an adversary following a certain sequence of actions [4–7, 10]. To assess the resilience of a facility to a threat, this modeling framework takes into account the most important factors specified in nuclear security recommendations by the International Atomic Energy Agency [9], including the detection, delay, response, and communication. In this chapter, we

---

E. Lykhovyd · S. Butenko (✉)

Wm. Michael Barnes '64 Department of Industrial and Systems Engineering, Texas A&M University, College Station, TX, USA

e-mail: [lykhovyd@tamu.edu](mailto:lykhovyd@tamu.edu); [butenko@tamu.edu](mailto:butenko@tamu.edu)

C. Marianno

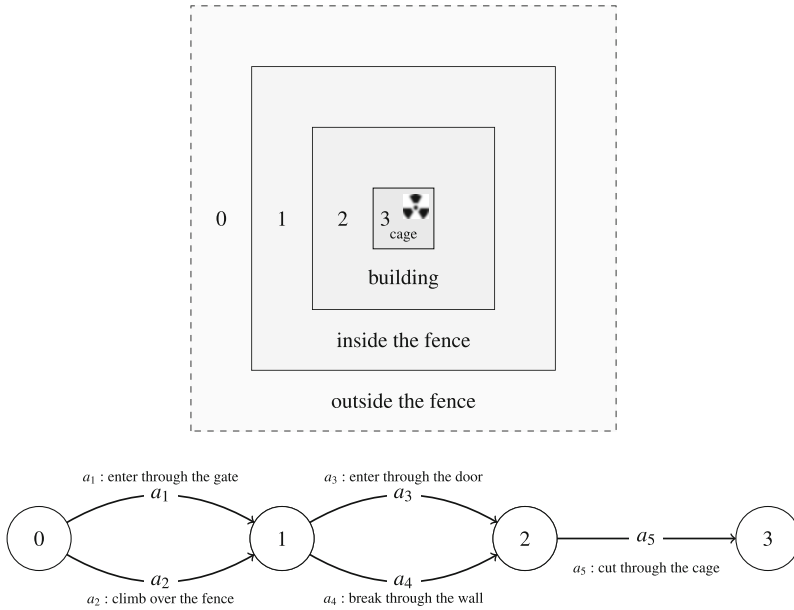
Department of Nuclear Engineering, Texas A&M University, College Station, TX, USA

e-mail: [marianno@tamu.edu](mailto:marianno@tamu.edu)

J. Yates

American Airlines, Fort Worth, TX, USA

e-mail: [justin.yates@aa.com](mailto:justin.yates@aa.com)



**Fig. 1** A network representation of a nuclear facility

follow this framework and specifically focus on making decisions concerning the first crucial component, that is, detection, aiming to maximize the resilience of a facility to potential threats under constrained budget.

We take advantage of a network representation of a nuclear facility, where the nodes correspond to different layers of security (such as outside the fence, inside the fence, inside the building, inside the cage) and the arcs model direct accessibility between the layers (i.e., getting inside the fence by entering through the gate or climbing over the fence; entering the building through the door or by breaking a wall, etc.). Figure 1 provides an illustration.

We assume that each arc can be enhanced by installing one or more detection or delay components from a given set of options. The corresponding objects (components, assets) are characterized by the following parameters: (1) detection probability; (2) delay time; and (3) associated cost. If the object already exists in the facility, for simplicity of the mathematical model we can either put its cost to 0 or force the corresponding object to be chosen in the model by setting to 1 the decision variable, indicating whether the object is selected (indeed, an object must be chosen if it benefits the security and comes at no cost). An example is given in Table 1. Upon detection of a threat, the system communicates with the responders (i.e., onsite guards or off-side troops) that will secure the area. This action is associated with the probability of successful communication (typically high, 0.9–0.99) and the time for response personnel to arrive.

**Table 1** A sample list of objects and their characteristics

Object	Detection probability	Delay time average	Delay time $\sigma$	Cost
Walkway to building	0	40 s	5 s	\$0
Front door	0.3	10 s	1 s	\$500
Inside camera	0.8	0	0	\$600

While we follow the EASI concept to create our mathematical model, in this work we limit ourselves to placing detection objects, assuming that the barriers and other delay objects are already presented in the facility.

The decisions we make regarding allocating the available budget to the detection components associated with the network's arcs determine the probability of detecting an adversary that follows a certain course of actions (path). Since the path a potential adversary will follow is not known in advance, we need to allocate the resources in a way that would minimize the overall system's vulnerability to a possible attack. In a robust optimization approach, one mitigates risks by planning for the worst-case scenario. That is, one allocates the budget so that the minimum probability of detecting a threat over all possible paths an adversary may take is as large as possible. Alternatively, one may use a more flexible risk-averse approach by optimizing or constraining some function that quantifies the risks by taking into account the risk preferences of the decision-maker.

In this work, we employ a modern risk measure called conditional value at risk (CVaR) to model risks associated with uncertainty in threat detection. This measure is closely related to value at risk (VaR), which essentially describes the maximum risk (loss function) value for a given percentage of worst-case scenarios. Given a parameter  $\alpha \in [0, 1]$ ,  $\alpha$ -CVaR is defined as the expected loss under the fraction  $(1 - \alpha)$  of the worst-case scenarios (see Fig. 2 for an illustration). This risk measure generalizes two popular approaches in risk management, optimizing the average risk (corresponds to  $\alpha = 0$ ) and the robust optimization approach, which is optimizing the worst-case outcome (corresponds to  $\alpha = 1$ ). Moreover, it gives the decision-maker a flexibility to balance between these two approaches and utilize the advantage of both of them while taking into account their risk preferences. In addition, unlike VaR, CVaR has appealing mathematical properties, such as sub-additivity and convexity, which are important in optimization modeling [14, 15]. All these factors made CVaR a popular choice in managing risks in various engineering applications [3, 11, 16], as well as in optimization modeling in networks subjected to uncertain nodes/arcs failures [2, 17].

The remainder of this chapter is organized as follows. The proposed models are formalized and solution algorithms are given in Sect. 2. The results of numerical experiments with sample networks are presented and discussed in Sect. 3. Finally, conclusion is made and directions for future work are outlined in Sect. 4.

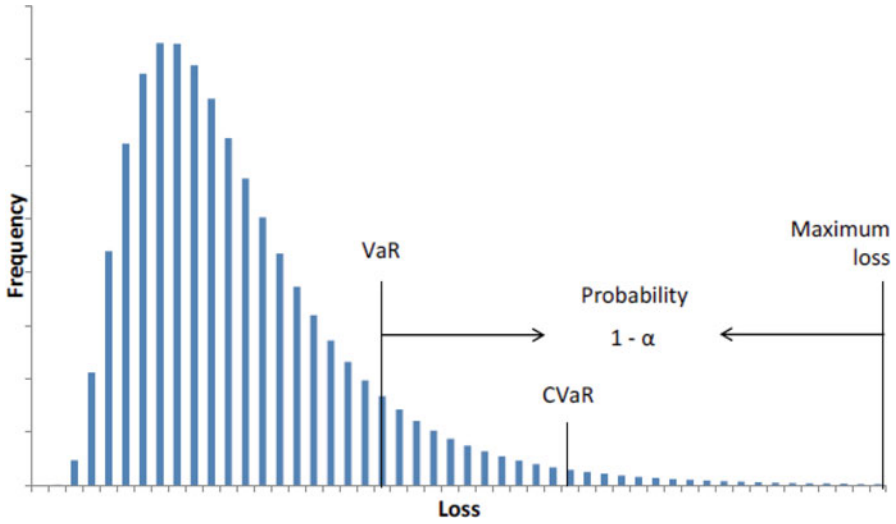


Fig. 2 A graphical illustration of VaR and CVaR

## 2 The Proposed Approach

Assume that the nuclear facility of interest is described as a network  $G = (N, A)$  where  $N$  is the set of nodes and  $A$  is the set of arcs. The adversary will try to get to the “core” of the facility. Thus, we assume that the attacker will try to follow some path from the outside of the facility to its core. We denote the starting node of the adversary path by  $s$  (source) and the last, target node by  $t$  (sink). Before describing the optimization models, we introduce the following notations.

Sets:

- $a \in A$ : arcs.
- $k \in K_a$ : available components for the arc  $a$ . “Do nothing” is included in  $K_a$  as a no-cost component.

Parameters:

- $B$ —the total available budget
- $c_a^k$ —the cost of component  $k \in K_a$  in arc  $a \in A$
- $p_a^k$ —the probability of detection for component  $k \in K_a$  in arc  $a \in A$
- $p_c$ —probability of successful communication with the responders
- $d_a^t$ —delay of reaching  $t$  from  $a$
- $d_c$ —responders’ time to arrival

For simplicity of exposition, we make the following assumptions.

**Assumption 1** Any two detection events with nonidentical indices (i.e., they differ in either  $a$  or  $k$ ) are independent of each other.

In general, this assumption is unnecessary as long as the probability of detection can be computed for a given arc and components configuration.

**Assumption 2** For each arc  $a$ ,  $K_a = \{0, 1, \dots, |K_a| - 1\}$  and the elements of  $K_a$  are monotonically ordered such that for  $k' < k''$  we have  $p_a^{k'} \leq p_a^{k''}$  and  $c_a^{k'} \leq c_a^{k''}$ . In particular,  $k = 0$  corresponds to the “do nothing” option with  $c_a^0 = 0$ .

If  $p_a^{k'} \leq p_a^{k''}$  but  $c_a^{k'} > c_a^{k''}$  for some  $k', k'' \in K_a$ , then it is always more reasonable to use the component  $k''$  because it is better in terms of detection probability and cheaper. Thus, the component  $k'$  never appears in the optimal solution and we can remove it from  $K_a$ .

For a given path from  $s$  to  $t$ , our point of interest is the probability of this path to withstand the adversary attack. For example, in a robust approach, we want to maximize the smallest such probability among all the possible paths.

We say the path fails if for each arc included in the path one of the following three conditions holds:

1. The arc fails to detect the adversary.
2. The arc detects the adversary, but fails to communicate this to the responders.
3. The arc detects the adversary and successfully communicates to the responders, but the responders’ time to arrival exceeds the adversary overall delay time of reaching the target from the current arc. Hence, the responders cannot stop the adversary in a timely fashion.

Thus, for a single arc  $a$  the probability to fail under configuration  $k$  is

$$p_{fail}^a = (1 - p_a^k) + p_a^k ((1 - p_c) + p_c \mathbb{1}_{\{d_a^t < d_c\}}). \tag{1}$$

Here the indicator  $\mathbb{1}_{\{d_a^t < d_c\}}$  is 1 if the adversary still cannot be stopped due to the poor response time of the security personnel (assuming that the arc detects the adversary and successfully communicates this to the responders), and 0, otherwise. To simplify the discussion, below we will assume that  $\mathbb{1}_{\{d_a^t < d_c\}} = 0$ , that is, responders always arrive on time.

A path  $\pi = (a_1, a_2, \dots, a_r)$  fails if every single arc in the path fails, so

$$P\{\text{path } \pi \text{ fails}\} = \prod_{i=1}^r p_{fail}^{a_i}. \tag{2}$$

We will follow the EASI concept to create the mathematical models. As mentioned above, in this work we limit ourselves to placing detection objects, assuming that the barriers and other delay objects are already present in the facility. The following two subsections present a robust and CVaR-based optimization model, respectively. The proposed formulations can be thought of as more complicated variations of the classical shortest path problem in networks [1].



### 2.1 Robust Optimization Model

In a robust optimization approach, we want to allocate the available budget such that the highest probability of any single path failing in the resulting system is as low as possible. We introduce the following decision variables:

$$x_{ij}^k = \begin{cases} 1, & \text{if the arc } (i, j) \text{ uses the detection element } k, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

Since “do nothing” is available as an option for each arc, we can assume that exactly one detection configuration needs to be picked for each arc, that is,

$$\sum_k x_{ij}^k = 1 \quad \forall (i, j). \tag{4}$$

Also, we cannot exceed the overall budget  $B$ :

$$\sum_{a=(i,j)} \sum_k c_a^k x_{ij}^k \leq B. \tag{5}$$

To specify the objective function, we will use the following auxiliary variables:

$$y_{ij}^k = \begin{cases} 1, & \text{if the arc } (i, j) \text{ with the detection element } k \text{ is in the worst path,} \\ 0, & \text{otherwise.} \end{cases} \tag{6}$$

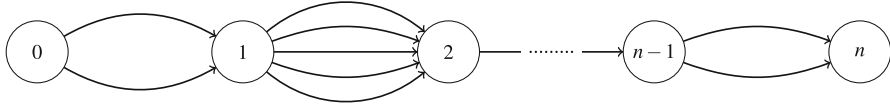
Then, since  $y_{ij}^k$  can be equal to 1 only if component  $k$  is selected for the arc  $(i, j)$ , we have

$$y_{ij}^k \leq x_{ij}^k \quad \forall k, (i, j). \tag{7}$$

Note that the model’s output is supposed to define a single path with the highest probability of failure under the configuration given by  $x$ . To ensure this, we use the conservation of flow constraints [1] in the form

$$\sum_k \left( \sum_j y_{ij}^k - \sum_j y_{ji}^k \right) = \begin{cases} 1 & \text{if } i = s \\ -1 & \text{if } i = t \\ 0 & \text{otherwise} \end{cases} \tag{8}$$

Let  $\pi$  be the path consisting of the arcs for which  $y_{ij}^k = 1$  for some  $k$ . Then our objective is to maximize  $\prod_{a \in \pi} p_{fail}^a$ , where  $p_{fail}^a = 1 - p_a^k + p_a^k(1 - p_c)$  for  $k$  with  $y_{ij}^k = 1$ . Taking the logarithm of this expression and denoting by  $w_a^k = -\log((1 - p_a^k) + p_a^k(1 - p_c))$ , we can write the objective as



**Fig. 3** A multi-arc path network

$$\max_x \min_y \sum_{a=(i,j)} \sum_k w_a^k y_{ij}^k. \tag{9}$$

The worst-case probability of failure of a path can be computed using the expression  $e^{-z^*}$ , where  $z^*$  is the optimal value of the model (3)–(9).

**The Case of a Multi-Arc Path Network**

Most nuclear facilities can be represented as a multi-arc path network (Fig. 3). This is the case when there are layers through which an adversary should move to reach sensitive elements. For example, in Fig. 1 such layers are outside the facility, inner outdoors area, inside the building, and inside the cage. Similar models are also typical for barrier placement; see [6] and Example 4 below.

To solve the robust optimization model for this case, we use dynamic programming to obtain a pseudo-polynomial algorithm for the robust path problem, drastically reducing the time needed to find an optimal solution.

We will call all arcs from node  $\ell$  to  $\ell + 1$  the *layer*  $\ell$ ; denoted by  $A_\ell$ . Then observe that the shortest path from 0 to  $n$  consists of the minimum-weighted arcs from each layer. The first step toward our final dynamic programming algorithm is a subroutine maximizing minimum arc weight in a layer with a given budget  $B_\ell$ . This subroutine can be solved with the following simple algorithm (Algorithm 1), using Assumption 2. The running time is  $O(|K_\ell|)$ , where  $K_\ell$  is the set of components that can be assigned to arcs in the layer, that is,  $K_\ell = \bigcup_{a \in A_\ell} K_a$ .

Now we are ready to present the dynamic programming algorithm. The idea is to compute the solution layer by layer for every budget. We store the previous result in array  $d[i, b]$  which denotes the solution for layers up to  $i$  and budget  $b$ . The algorithm can be implemented to run in  $O(|V| \cdot |K_\ell| \cdot B)$  time [13].

**2.2 CVaR-Based Model**

Next, we propose a model that, instead of minimizing the probability of failure of the worst path, minimizes the risk expressed in terms of CVaR for the loss function given by the probability of a path failure for a given configuration. To demonstrate potential advantages of a CVaR-based approach over a robust optimization model,

---

**Algorithm 1** Subroutine for optimally allocating budget  $B_\ell$  to layer  $\ell$

---

```

SolveLayer( $A_\ell, B_\ell$ )
 $k_a = 0, a \in A_\ell$                                 ▷ component selected for arc  $a$ 
 $budget \leftarrow B_\ell$                             ▷ available budget
while  $budget > 0$  do
     $LB \leftarrow \min_{a \in A_\ell} p_a^{k_a}$                 ▷ the lowest probability of detection among the layer's arcs
     $A_\ell^{\min} = \{a \in A_\ell : p_a^{k_a} = LB\}$         ▷ arcs with the lowest probability of detection in the layer
    if  $\sum_{a \in A_\ell^{\min}} c_a^{k_a+1} \leq budget$  then
        for every arc  $a \in A_\ell^{\min}$  do
             $k_a = k_a + 1$                             ▷ choose the next (better) component for each arc in  $A_\ell^{\min}$ 
        end for
    end if
     $budget = budget - \sum_{a \in A_\ell^{\min}} c_a^{k_a}$         ▷ update the available budget
end while
return  $LB$ 

```

---



---

**Algorithm 2** Dynamic programming algorithm for a multi-arc path network

---

```

DynRobust( $B, G = (V, E)$ )
 $d[0, b] \leftarrow 0$  for  $b = 0, \dots, B$ 
for  $i = 1, \dots, |V|$  do
    for  $b_1 = 0, \dots, B$  do
        for  $b_2 = 0, \dots, b_1$  do
             $d[i, b_1] \leftarrow SolveLayer(b_1 - b_2, i) + d[i - 1, b_2]$ 
        end for
    end for
end for
return  $d[|V|, B]$ 

```

---

**Table 2** Possible output of the robust optimization and CVaR-based models for the same example

	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$	$P_7$
Robust	0.09	0.09	0.09	0.09	0.09	0.09	0.09
CVaR	0.10	0.01	0.01	0.01	0.01	0.01	0.01

consider a hypothetical network with seven possible paths from source to sink, with results obtained using both approaches presented in Table 2. More specifically, the table presents the probability of an adversary to succeed for each of the seven paths for the robust and CVaR-based approaches, respectively. We observe that with the robust solution every path has the same probability 0.09 of failure, whereas CVaR-based solution has a slightly less secure most vulnerable path, but much more secure remaining paths compared to the robust solution. In the case when there are many adversary paths, one might see the CVaR-based approach as a more appropriate method for placing security devices.

To develop an algorithm for optimizing CVaR, observe that the loss function can be equivalently thought of as a length of the corresponding path with arc weights given by  $w_a^k$ 's described above. Then minimizing CVaR is equivalent to maximizing

the average of the fraction  $\alpha$  of the shortest paths. The procedure for finding an optimal solution to the problem is described in Algorithm 3.

---

**Algorithm 3** Finding optimal solution for the CVaR-based model

---

```

 $p_{min} \leftarrow 1$ 
for every configuration  $x$  do
    if  $x$  satisfies the budget then
        compute fraction  $\alpha$  paths from  $s$  to  $t$  with the minimum weight
        compute the average probability from weights as  $p$ 
        if  $p < p_{min}$  then  $p_{min} \leftarrow p$ 
        end if
    end if
end for
return  $p_{min}$ 
    
```

---

The algorithm uses the depth-first search (DFS) subroutine described in Algorithm 4 to find all paths from  $s$  to  $t$ . Here the variable `cur` stores the current weight of the path being constructed, the variable `pathnumber` contains the number of paths detected so far, and the array `weights` saves the weight of each path.

---

**Algorithm 4** Depth-first search

---

```

DFS( $v, t, cur, weights$ )
 $cur \leftarrow 0$ ;  $pathnumber \leftarrow 0$ ;  $weights \leftarrow []$ 
for every arc  $(v, u)$  do
     $cur \leftarrow cur + weight(v, u)$ 
    if  $u = t$  then
         $pathnumber \leftarrow pathnumber + 1$ 
         $weights[pathnumber] \leftarrow cur$ 
    else
        DFS( $u, t, cur, weights$ )
    end if
end for
DFS( $s, t, 0, \emptyset$ )
    
```

---

### 3 Case Studies

The program producing the IP described above was created using GNU C++11 and solved using CPLEX v12.6.3. The host machine used Intel(R) Xeon(R) CPU @ 2.40 GHz, 11 GB RAM. The CVaR-based approach was compared against the robust optimization formulation on four sample instances presented in the following four subsections. The results for each example are summarized in a table in each corresponding subsection, which, for a given budget, contains the probability  $P$

of a successful adversary attack along the most vulnerable path for the robust approach, and the average probability of a successful attack along fraction  $\alpha$  of most vulnerable paths for the CVaR-based approach. If the two approaches resulted in different choices of detection components, the corresponding values are shown in bold.

### 3.1 Example 1

We consider a simple network given in Fig. 4. The data for the input files can be found in Appendix “Input Data for Example 1”. We assume that the barriers have infinite delay time. Since there are only two alternative paths from node 0 to node 4 in this network, the CVaR approach is equivalent to the robust optimization method for any  $\alpha \in (0, 1]$  and optimizes the expected probability of adversary success when  $\alpha = 0$ . Therefore,  $\alpha = 0$  is considered, which is equivalent to minimizing the average probability.

Tables 3 and 4 and Fig. 5 present the results and a graphical comparison of optimal objective values as a function of budget for the two approaches.

We observe that the budget increase is particularly beneficial when the overall budget is low, whereas improvement in the objective becomes insignificant with higher budget levels. Setting the budget that allows implementing the best available option for each arc, we obtain the optimal value with the adversary success

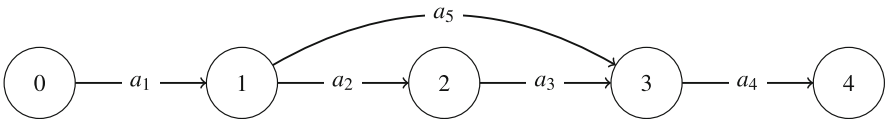


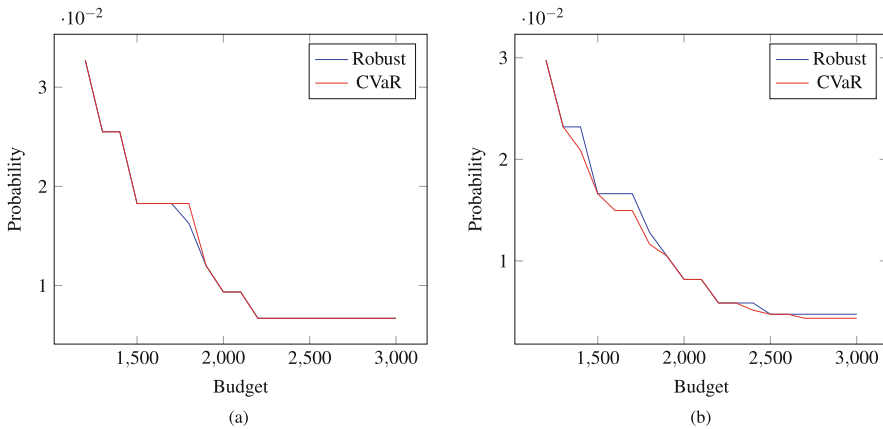
Fig. 4 The network of adversary paths used in Example 1

Table 3 Results table for Example 1

Budget	1200	1400	1600	1800	2000	2200	2400	2600	2800	3000
Robust	0.033	<b>0.026</b>	<b>0.018</b>	<b>0.016</b>	0.009	0.007	<b>0.007</b>	0.007	<b>0.007</b>	<b>0.007</b>
CVaR	0.030	<b>0.021</b>	<b>0.015</b>	<b>0.012</b>	0.008	0.006	<b>0.005</b>	0.005	<b>0.004</b>	<b>0.004</b>

Table 4 Decisions comparison between robust and CVaR approaches for budget  $B = 1800$

	Arc	$a_1$	$a_2$	$a_3$	$a_4$	$a_5$
Robust	Component	Camera1	Camera1	<i>nothing</i>	CameraX	CameraX
	Probability	0.7	0.7	0	0.9	0.85
	Price	300	300	0	600	600
CVaR	Component	Camera2	Camera1	Camera3	CameraX	Camera3
	Probability	0.8	0.7	0.6	0.9	0.5
	Price	500	300	200	600	200



**Fig. 5** Results obtained using the robust optimization method and the CVaR-based approach for Example 1. (a) Worst path value. (b) CVaR value

**Table 5** Results table for Example 2

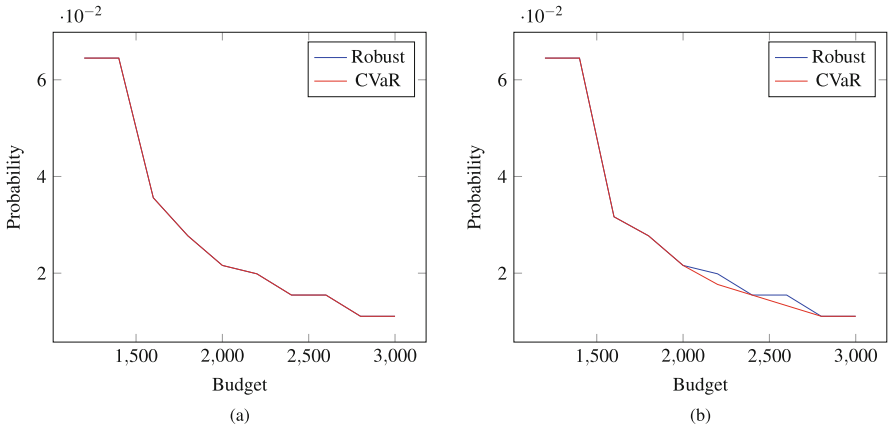
Budget	1200	1400	1600	1800	2000	2200	2400	2600	2800	3000
Robust	0.064	0.064	0.036	0.028	0.022	<b>0.020</b>	0.015	<b>0.015</b>	0.011	0.011
CVaR	0.064	0.064	0.032	0.028	0.022	<b>0.018</b>	0.015	<b>0.013</b>	0.011	0.011

probability being  $P_1(\text{success}) = 0.0043 = 0.43\%$ . Reducing the budget to \$1200, the probability of the adversary success becomes  $P_1(\text{success}) = 0.029 = 2.9\%$ . The optimal objective for the CVaR-based approach is always smaller since it is given by the average over the two possible adversary paths rather than the worst path.

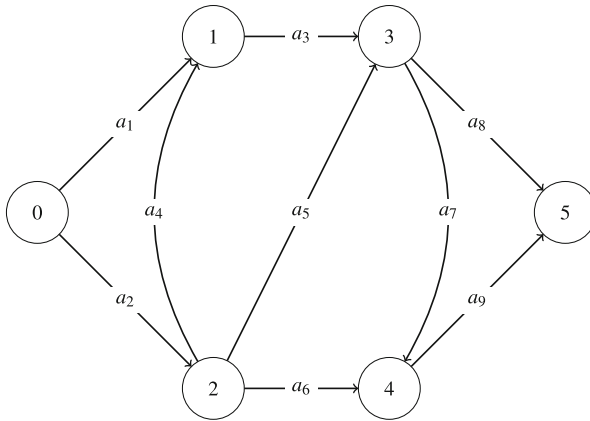
In addition, from Table 3 one might observe that when the budget is high, opposite to CVaR, robust approach stops optimizing remaining adversary paths.

### 3.2 Example 2

The second example we consider deals with the network in Fig. 1. The CVaR-based approach was applied with  $\alpha = 0.5$ , which corresponds to optimizing the average security for two worst paths out of the total of four paths. Table 5 shows the probability of a successful adversary attack for different budget levels produced by robust paths and CVaR methods. These results are illustrated graphically in Fig. 6.



**Fig. 6** Results obtained using the robust optimization method and the CVaR-based approach for Example 2. (a) Worst path value. (b) CVaR value



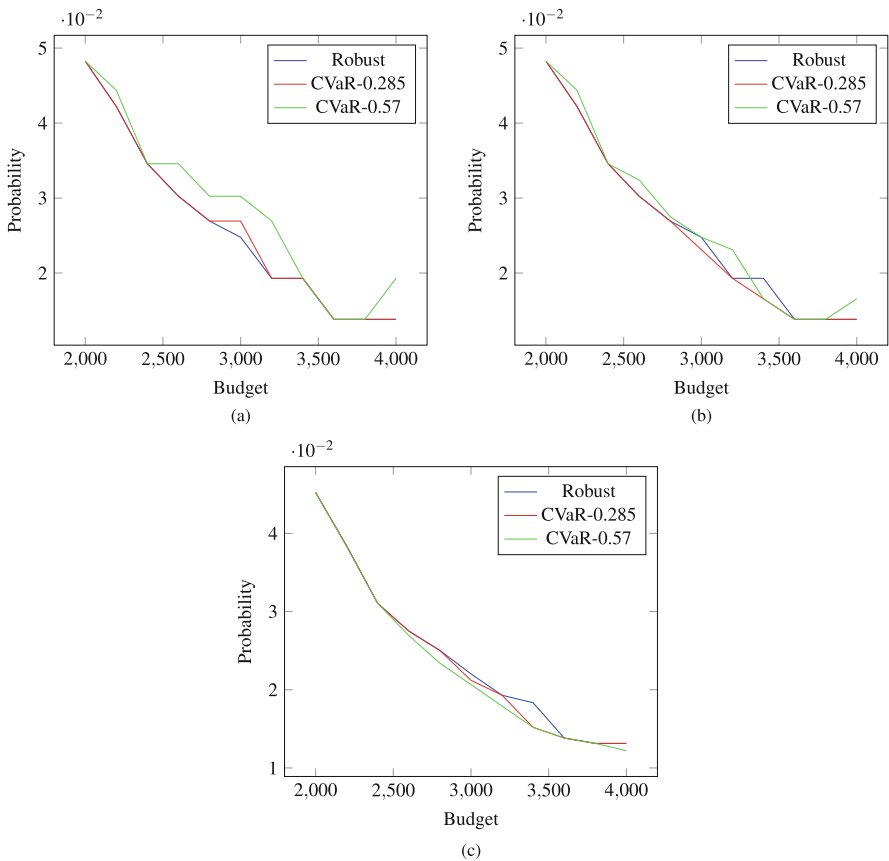
**Fig. 7** The network used in Example 3

### 3.3 Example 3

In the next example, we consider a more sophisticated network presented in Fig. 7. The network has seven different adversary paths. For the CVaR-based approach, we optimize over 2 and 4 worst paths, which corresponds to  $\alpha \approx 0.285$  and  $\alpha \approx 0.57$ , respectively. The results are shown in Table 6 and Fig. 8. In Table 6, the cases where the decision was different from robust approach are shown in bold, while the cases where the decision for CVaR-0.57 was different from CVaR-0.285 are shown in italic.

**Table 6** Results table for Example 3

Budget	2000	2300	2600	2900	3200	3500	3800	4100
Robust	0.048	<b>0.042</b>	0.030	<b>0.027</b>	0.019	<b>0.019</b>	0.014	0.014
CVaR-0.285	0.048	<b>0.039</b>	0.030	<b>0.026</b>	0.019	<b>0.017</b>	0.014	0.014
CVaR-0.57	0.045	<i>0.034</i>	<b>0.027</b>	<b>0.022</b>	<b>0.018</b>	<b>0.015</b>	0.013	<b>0.011</b>



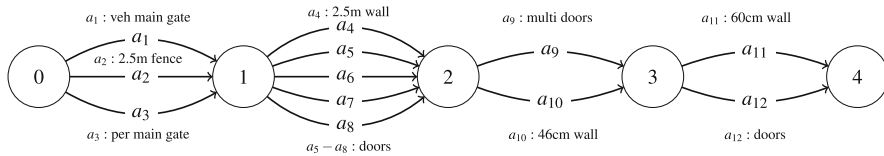
**Fig. 8** Results obtained using the robust optimization method and the CVaR-based approach for Example 3. (a) Worst path value. (b) CVaR-0.285 value. (c) CVaR-0.57 value

In addition, Table 7 shows the optimal solution produced by robust approach and CVaR for the budget of \$3500. In this table, we show the probability of an adversary to succeed along every possible path. Recall the focus of the CVaR risk measure. It returns the average of the worst paths. So, minimizing CVaR results in decisions that optimize the resilience of some subset of worst paths. In the considered example, while the robust optimization and CVaR decisions result in worst paths of the same quality, the latter approach tends to have more balanced remaining paths. In



**Table 7** Comparison of the robust optimization and CVaR-based approaches for  $B = \$3500$

	$P_1$	$P_2$	$P_3$	$P_4$	$P_5$	$P_6$	$P_7$
Robust	0.019	0.019	0.019	0.015	0.006	0.006	0.005
CVaR	0.019	0.013	0.013	0.013	0.013	0.011	0.011



**Fig. 9** A network representation of a nuclear facility from [6]

particular, its second, third and fourth worst paths are more secure than those for the robust approach.

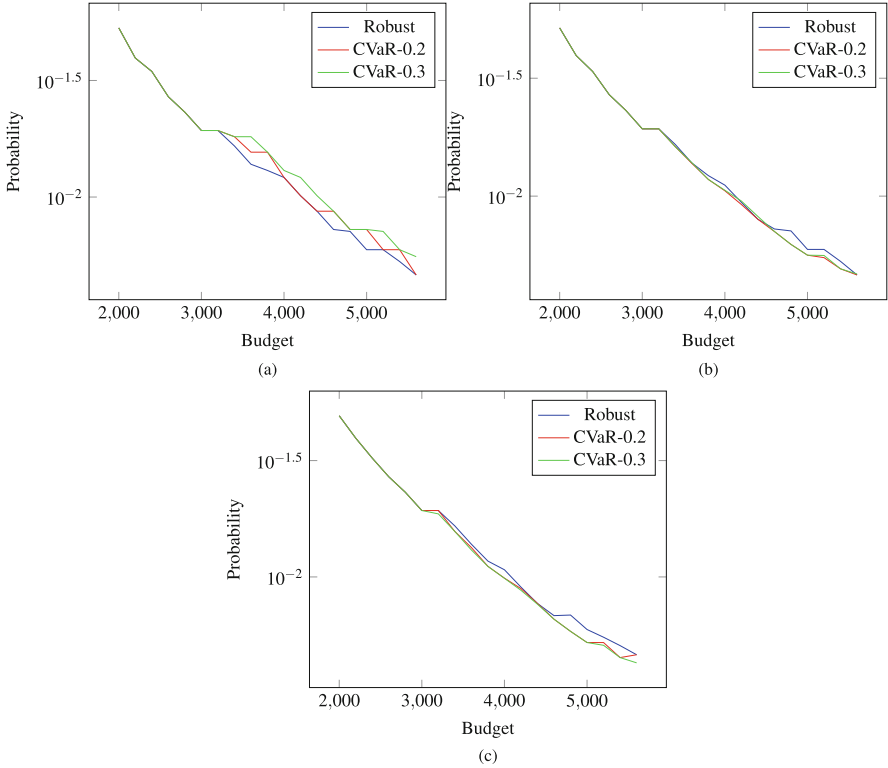
### 3.4 Example 4

The last considered example is borrowed from a previously published study [6], where the delay component analysis was presented. Here we model the assignment of detection components using the data presented in Appendix “Input Data for Example 4”. The corresponding network representation of the facility is shown in Fig. 9. There are 12 arcs and  $3 \times 5 \times 2 \times 2 = 60$  paths. We consider  $\alpha = 0.2$  and  $\alpha = 0.3$ , which corresponds to 12 and 18 most vulnerable paths out of 60 (Fig. 10).

In this example due to small  $\alpha$  for CVaR and similar components for arcs, robust approach decisions are almost identical to CVaR-based decisions (Table 8).

## 4 Conclusion and Future Work

In this chapter, we described the foundation of the network-based risk-averse approach to solving nuclear security decision problems. The natural extensions could include the barrier placement decision, different security personal placements, and more. Also, one might want to model the dependencies of the probabilities on certain factors, for example, the communication probability could vary depending on the arc instead of being constant, detection probabilities might depend on other camera placements, etc. The proposed approach could be naturally extended to include all cases mentioned above.



**Fig. 10** Results obtained using the robust optimization method and the CVaR-based approach for Example 4. (a) Worst path value. (b) CVaR-0.2 value. (c) CVaR-0.3 value

**Table 8** Results table for Example 4

Budget	2000	2400	2800	3200	3600	4000	4400	4800	5200	5600
Robust	0.053	0.035	0.023	0.019	0.014	0.012	0.009	0.007	0.006	0.005
CVaR-0.2	0.052	0.034	0.023	0.019	0.014	0.011	0.008	0.006	0.005	0.005
CVaR-0.3	0.049	0.032	0.023	0.019	0.013	0.010	0.008	0.006	0.005	0.004

## Appendix

### *Input Data for Example 1*

```
# communication prob
0.95
#budget
1000.0
#s and t
0 4
```

```

# Available Components
# please no comments later, only empty lines
# must have the next line
-----
Camera1 0.7 300 a1
Camera2 0.8 500 a1
Camera3 0.6 200 a1

Camera1 0.7 300 a2
Camera2 0.8 500 a2

Camera2 0.8 500 a3
Camera3 0.6 200 a3

Camera1 0.7 300 a4
CameraX 0.9 600 a4

Camera3 0.5 200 a5
CameraX 0.85 600 a5

```

### Graph Data

```

n 5 5
e 0 1 a1
e 1 2 a2
e 2 3 a3
e 3 4 a4
e 1 3 a5

```

### *Input Data for Example 2*

The object data is the same as for Example 3.

### Graph Data

```

n 4 5
e 0 1 a1
e 0 1 a2
e 1 2 a3
e 1 2 a4
e 2 3 a5

```

***Input Data for Example 3***

```
# communication prob
0.95
#budget
3800
#s and t
0 5
# Available Components
# please no comments later, only empty lines
# must have the next line
-----
Camera1 0.7 300 a1
Camera2 0.8 500 a1
Camera3 0.6 200 a1

Camera1 0.7 300 a2
Camera2 0.8 500 a2

Camera2 0.8 500 a3
Camera3 0.6 200 a3

Camera1 0.7 300 a4
CameraX 0.9 600 a4

Camera3 0.5 200 a5
CameraX 0.85 600 a5

Camera1 0.7 300 a6
Camera2 0.8 500 a6
Camera3 0.6 200 a6

Camera1 0.7 300 a7
Camera2 0.8 500 a7
Camera3 0.6 200 a7

Camera1 0.7 300 a8
Camera2 0.8 500 a8
Camera3 0.6 200 a8

Camera1 0.7 300 a9
Camera2 0.8 500 a9
Camera3 0.6 200 a9
```

**Graph Data**

```

n 6 9
e 0 1 a1
e 0 2 a2
e 1 3 a3
e 2 1 a4
e 2 3 a5
e 2 4 a6
e 3 4 a7
e 3 5 a8
e 4 5 a9

```

***Input Data for Example 4***

```

# communication prob
0.95
#budget 1200.0 as min
3600
#s and t
0 4
# Available Components
# please no comments later, only empty lines
# must have the next line
-----
Camera1 0.7 300 a1
Camera2 0.8 500 a1
Camera3 0.6 200 a1

Camera1 0.7 300 a2
Camera2 0.8 500 a2
CameraX 0.9 600 a2

Camera1 0.5 100 a3
Camera2 0.8 500 a3
Camera3 0.6 200 a3

Camera1 0.7 300 a4
CameraX 0.9 600 a4

Camera3 0.5 200 a5
Camera2 0.7 400 a3
CameraX 0.85 600 a5

```

Camera1 0.75 300 a6  
Camera2 0.8 500 a6  
Camera3 0.6 200 a6

Camera1 0.7 300 a7  
Camera2 0.8 500 a7  
Camera3 0.65 200 a7

Camera1 0.7 300 a8  
Camera2 0.85 500 a8  
Camera3 0.6 200 a8

Camera1 0.75 300 a9  
Camera2 0.8 500 a9  
Camera3 0.65 200 a9

Camera1 0.7 300 a10  
Camera2 0.8 500 a10  
Camera3 0.85 600 a10

Camera2 0.8 500 a11  
Camera3 0.6 200 a11

Camera1 0.7 300 a12  
Camera2 0.8 500 a12  
CameraX 0.9 600 a12

**Graph Data**

n 5 12  
e 0 1 a1  
e 0 1 a2  
e 0 1 a3  
e 1 2 a4  
e 1 2 a5  
e 1 2 a6  
e 1 2 a7  
e 1 2 a8  
e 2 3 a9  
e 2 3 a10  
e 3 4 a11  
e 3 4 a12

## References

1. Ahuja, R.K., Magnanti, T.L., Orlin, J.B.: *Network Flows: Theory, Algorithms, and Applications*. Prentice-Hall, Englewood Cliffs (1993)
2. Boginski, V.L., Commander, C.W., Turko, T.: Polynomial-time identification of robust network flows under uncertain arc failures. *Optim. Lett.* **3**(3), 461–473 (2009)
3. Cholda, P., Følstad, E.L., Helvik, B.E., Kuusela, P., Naldi, M., Norros, I.: Towards risk-aware communications networking. *Reliab. Eng. Syst. Saf.* **109**, 160–174 (2013)
4. Garcia, M.L.: *The Design and Evaluation of Physical Protection Systems*, 2nd edn. Sandia National Laboratories (2007)
5. Gordon, K.A., Wyss, G.D.: Comparison of two methods to quantify cyber and physical security effectiveness. Technical Report SAND2005-7177, Sandia National Laboratories, 2005
6. Hawila, M.A., Chirayath, S.S.: Combined nuclear safety-security risk analysis methodology development and demonstration through a case study. *Progr. Nucl. Energy* **105**, 153–159 (2018)
7. Hromada, M., Lukas, L.: Critical infrastructure protection and the evaluation process. *Int. J. Disaster Recovery Bus. Continuity* **3**, 37–46 (2012)
8. Institute for Nuclear Materials Management. Global best practices for physical protection (2004). [https://www.inmm.org/Physical\\_Protection.htm](https://www.inmm.org/Physical_Protection.htm). Last accessed in December 2016
9. International Atomic Energy Agency. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/revision 5) : Recommendations (2010). [http://www-pub.iaea.org/mtcd/publications/pdf/pub1481\\_web.pdf](http://www-pub.iaea.org/mtcd/publications/pdf/pub1481_web.pdf)
10. Lukas, L., Hromada, M.: Utilization of the EASI model in the matters of critical infrastructure protection and its verification via the OTB SAF simulation tool. In: 13th WSEAS International Conference on AUTOMATIC, pp. 131–136. Canary Islands, Spain (2011)
11. Mínguez, R., Conejo, A.J., García-Bertrand, R.: Reliability and decomposition techniques to solve certain class of stochastic programming problems. *Reliab. Eng. Syst. Saf.* **96**(2), 314–323 (2011)
12. Office of the Deputy Assistant Secretary of Defense for Nuclear Matters. Nuclear Matters Handbook 2016. [http://www.acq.osd.mil/ncbdp/nm/NMHB/chapters/chapter\\_7.htm](http://www.acq.osd.mil/ncbdp/nm/NMHB/chapters/chapter_7.htm)
13. Pferschy, U.: Dynamic programming revisited: improving knapsack algorithms. *Computing* **63**(4), 419–430 (1999)
14. Rockafellar, R.T., Uryasev, S.: Optimization of conditional value-at-risk. *J. Risk* **2**(3), 21–41 (2000)
15. Rockafellar, R.T., Uryasev, S.: Conditional value-at-risk for general loss distributions. *J. Bank. Financ.* **26**(7), 1443–1471 (2002)
16. Seyedshohadaie, S.R., Damnjanovic, I., Butenko, S.: Risk-based maintenance and rehabilitation decisions for transportation infrastructure networks. *Transport. Res. A* **44**, 236–248 (2010)
17. Yezeraska, O., Butenko, S., Boginski, V.: Detecting robust cliques in graphs subject to uncertain edge failures. *Ann. Oper. Res.* (2016). <https://doi.org/10.1007/s10479-016-2161-0>

# Post-Disaster Damage Assessment Using Drones in a Remote Communication Setting



Ecem Yucesoy, Elvin Coban, and Burcu Balcik

## 1 Introduction

Over the last twenty years, the number and impact of disasters have increased drastically with 7348 recorded disaster events, which affected more than 4 billion people and caused approximately 1.23 million deaths [11], which underline the increased importance of effective disaster management. Although preparedness efforts are known to bring the most benefits to minimizing the adverse effects of a disaster [46], well-planned and effectively organized emergency response operations, especially within the first hours, are critical for saving lives. In particular, rapid damage assessment operations are vital for humanitarian organizations to identify and serve disaster victims in need effectively [27].

The recent advances in technologies create opportunities to mitigate and prepare for disasters and respond faster. One technology that provides several advantages to pre-disaster and post-disaster operations is unmanned aerial vehicles (UAVs), which are also called drones. Since obtaining accurate data quickly during disaster management operations is crucial, the use of drones for these operations has become widespread recently. Drones provide many advantages during response operations, such as shortening the required time to discover victims since they can explore a vast area in a short time, providing information regarding the route to take for rescue teams, and identifying alive victims trapped under rubble by using noise sensing, binary sensing, vibration sensing, and heat-sensing features [13]. Usage areas of drones for disaster management include, but are not limited to, monitoring, information generation and sharing, situational awareness, evacuation, stand-alone communicating system, search and rescue operations, and damage assessment [17].

---

E. Yucesoy · E. Coban · B. Balcik (✉)

Industrial Engineering Department, Ozyegin University, Istanbul, Turkey

e-mail: [ecem.yucesoy@ozu.edu.tr](mailto:ecem.yucesoy@ozu.edu.tr); [elvin.coban@ozyegin.edu.tr](mailto:elvin.coban@ozyegin.edu.tr); [burcu.balcik@ozyegin.edu.tr](mailto:burcu.balcik@ozyegin.edu.tr)



Even though drones provide many advantages to disaster management operations, there exist challenges to deal with while using drones, such as the limited battery capacity and flight range, as well as legal and ethical considerations.

Although drone technology is relatively new, drones have already been utilized after several recent disasters to support assessment activities. For example, drones were used for 3D mapping of the area during the California campfire in 2018 [23], and in rescue services for the fire activities in the United Kingdom [34]. After hurricanes Harvey, Irma, and Florence in 2017, 2017, and 2018 respectively, drones were used for damage assessment and were found to be practical, safer, and less expensive compared to the traditional manned aerial inspection [39]. Drones assisted with flood mapping activities in Dar es Salaam in 2018, and spatial modeling of displaced landmines after the 2014 Bosnia-Herzegovina floods [22]. Moreover, drones were used for mapping purposes to identify the damage after the earthquakes in Nepal in 2015, Haiti in 2010, Ecuador in 2016 [22], and Petrinja in 2020 [15].

Most use cases of drones for disaster management operations require drones to systematically hover over a certain area, creating the need to construct drone routes. Since speed is an important factor for damage assessment operations, optimal or near-optimal routes should be determined quickly, considering the characteristics and aim of the task. Problems where drones are utilized for disaster management operations have been widely studied recently in the operations research literature. So far, the existing studies have focused on the transportation and delivery, surveying and monitoring, and communication and integration capabilities of drones. However, since this is a relatively new area, there exist numerous important features related to the usage of drones that needs to be further explored. For example, as highlighted by Rejeb et al. [42], investigating the data collection activities of drones is important for surveying and monitoring purposes. Moreover, from a technological perspective, examining the real-life limitations of drones (e.g., battery levels, recharging times, communication ranges) in different problem settings (such as path planning, scheduling, and task assignment) would contribute to the literature.

In this study, we are motivated by using drones for damage assessment in an earthquake-affected area and investigate a setting where remote data transmission by drones is possible as they scan the region. The affected area is assumed to be divided into grids with different criticality levels. Moreover, there exists an operation center where the transmitted information is analyzed and the drones initially take off. Since drones have a limited battery capacity, we consider recharge stations (RSs) that are located on certain grids. Drones have to visit the RSs to recharge their batteries as required along their route. An exemplary network that shows drone routes is provided in Fig. 1.

The online setting brings two advantages to disaster management operations compared to an offline setting where en-route information transmission is not possible and drones can transmit information only at the end of the assessment horizon after they return to the operation center [1]. Firstly, in the online setting, the information regarding the situation of the scanned grids can be sent to the operation center faster, decreasing the response time to these grids. Secondly, since the drone

can recharge and transmit data without the need to return to the operation center, more grids can be assessed within a shorter period of time.

We consider an online setting where drones can remotely transmit the footage that is obtained by scanning the areas. In this online setting, we assume that the data transmission will only occur at the grids that include an RS. After a disaster, the communication infrastructure in the affected area can be damaged in some parts of the network. For instance, after the Indian Ocean tsunami in 2004, the telecommunication infrastructure was severely damaged, and there was an immediate reconstruction of infrastructure to improve data collection and decision-making infrastructure as part of the response operations [38]. After the earthquake in Kobe, Japan, in 1995, the communication failures caused significant delays in the response operations under harsh weather conditions since the severity of damage was unknown [47]. Khaled and Mcheick [29] review the communication systems and their weaknesses under harsh environments, such as the New York City WTC attacks in 2001, the Indian Ocean earthquake in 2004, the Haiti earthquake in 2010, and the Nepal earthquake in 2015. The recovery of telecommunications from several disasters, such as the earthquakes in Christchurch in 2011, Maule in 2010, and the Indian Ocean in 2004, is analyzed and modeled in [50]. In our setting, we assume that a partially reconstructed infrastructure is available; that is, drones can transmit information in all or some of the RS grids in the network. This is a reasonable assumption since a temporary portable communication network can be established at the RS grids for this purpose, which is a common approach in post-disaster settings [47].

We aim to present a mathematical model that support constructing optimal or near-optimal routes for drones in order to assess a disaster-affected area systematically and gather information quickly by considering a setting with remote data transmission. The collected damage assessment information is critical for all upcoming time-sensitive disaster relief activities, such as search and rescue operations. Formulating and solving such a routing problem by considering several important factors (such as the different criticality levels of the affected areas, battery limitations of drones, and different routing characteristics of the communication settings) is quite challenging. To address this challenge, we propose a path-based formulation, which is adapted from Adsanver et al. [1], in which the authors show that the path-based formulation performs better than the arc-based formulation for a similar drone routing problem. In the path-based formulation, the routing decisions are made based on the selection of path segments (see Fig. 2) to reduce the number of decision variables and enhance the performance of the model. In our mixed integer linear programming (MILP) model, we maximize the total priority scores obtained from the visited grids within an assessment horizon to facilitate assessing urgent areas quickly while reducing the response time for the assessed grids. We present computational results to test the proposed MILP and conduct sensitivity analysis on randomly generated instances to explore the benefits of an online setting compared to a setting where data transmission is only possible at the end of the routes.

The rest of this chapter is organized as follows. In Sect. 2, we review the related literature. In Sect. 3, we define the drone routing problem with remote communication (DRP-RCOM) and introduce our mathematical model. In Sect. 4, we present the test instances, propose the performance metrics, and discuss the results. Finally, we give concluding remarks in Sect. 5.

## 2 Literature Review

Our study is related to the stream of literature that focuses on drone route planning problems in the context of humanitarian assessment operations. In this section, the studies that focus on drone usage in humanitarian operations and the related vehicle routing problems (VRPs) are briefly reviewed. For a more detailed review of routing problems with drones, the reader is referred to Macrina et al. [36].

### 2.1 Drones in Humanitarian Operations

The number of studies that focus on drone-aided humanitarian logistics has grown drastically over the past ten years. One of the most commonly studied areas of use for drones is post-disaster assessment operations. The primary aim of the assessment operations is to rapidly collect information for damage detection. We first review the relevant example studies that focus on modeling and solving drone routing problems to assist damage assessment operations and then provide examples that focus on using drones to assist humanitarian operations in different ways.

Oruç and Kara [37] address using drones and motorcycles to assist post-disaster assessment operations. The authors consider the importance of road segments and population points and present  $\epsilon$ -constraint and heuristic methods to solve the proposed bi-objective model. In [10], the authors aim to find optimal routes and trajectories of a fleet of gliders to survey a set of locations. Similarly, the flight dynamics of gliders are considered, and the solution methods are tested in a case study. Zhu et al. [49] solve a variant of the team orienteering problem that constructs the assignment plan for multiple drones in a rapid-assessment task with a hybrid particle swarm optimization algorithm with simulated annealing. While assigning tasks to drones, the authors consider the weights of potential targets, the endurance of the drones, and the sensor errors. Worden et al. [48] solve a task assignment problem with drones, where the aim is to maximize the information gain from the scanned damage-affected areas. The authors consider a setting in which drones are able to communicate with the control station at all times, and there exist limitations regarding data broadcast. Adsanver et al. [1] focus on the drone routing problem for the assessment of a disaster-affected area that is divided into grids, where the grids are clustered based on different attributes. The authors define an offline setting, where no en-route data transfer is considered, and they compare two

different, arc-based and path-based, formulations in terms of run-time performance. Chowdhury et al. [9] define a Heterogeneous Fixed Fleet Drone Routing problem to minimize the post-disaster inspection cost, while the drone-specific features are taken into account. The problem is solved with adaptive large neighborhood search and modified backtracking adaptive threshold accepting algorithms and tested on a real-life case study.

Assessing the infrastructure network conditions and accessibility with drones is also beneficial while planning the distribution of relief goods with ground vehicles. Macias et al. [35] present a stochastic vehicle routing problem, where the drones determine the damaged infrastructure and ground vehicles are simultaneously routed. The authors present results that highlight the benefit of using drones for assessment. Reyes-Rubiano et al. [43] propose an online routing algorithm for drones to detect disruptions on the road network after a disaster. The authors assume that the information obtained with drones are sent to the operation center with real-time video, and based on the detected disruptions, the drones are re-routed with an exploration strategy.

An important goal of the post-disaster damage assessment operations is to support the search and rescue operations by locating disaster victims. Bravo et al. [6] solve an area coverage problem to find the victims based on a Partially Observable Markov Decision Process. The algorithm considers the information collected so far with the drones to update the likelihood of finding victims in different areas and make routing decisions accordingly. Ejaz et al. [16] focus on an energy-efficient task scheduling scheme for data collection with drones, where drones are equipped with necessary sensors and can analyze the vital signs data collected from the victims. The areas are prioritized based on the health risk status of the victims, which is classified with a decision tree algorithm. In [26], the authors suggest incorporating the tornado weather data into search and rescue procedures and create drone routes accordingly to minimize the time span. Similarly, [31] focus on a search and rescue mission with drones, with the aim of minimum latency, where the disaster-affected area is assumed to be divided into grids. Different objectives are tested, and heuristic algorithms are analyzed as the solution methods.

The distribution of small-sized relief goods, such as vaccines, blood, and water-sanitizer tablets, is another area where drones are used in the aftermath of a disaster. Chowdhury et al. [8] propose a continuous approximation model to determine the optimal distribution center locations, where the relief goods can be distributed with drones or trucks. Similarly, Golabi et al. [24] study a stochastic combined mobile and immobile facility location problem to locate the relief distribution centers after an earthquake. The authors assume that drones will deliver relief items to the recipients that are at inaccessible edges. Fikar et al. [19] focus on developing a simulation and optimization-based decision support system to carry the coordination of transportation of relief items via drones or off-road vehicles. A MIP formulation, agent-based simulation, and heuristic algorithms are proposed to solve the scheduling and routing problem. Rabta et al. [40] focus on the last-mile delivery of multiple small packages with drones as well, where experiments are conducted under different prioritization schemes of nodes.

Besides the previously mentioned use cases, drones are also deployed to support the damaged communication structure as temporary base stations, with the examples of Sharafeddine and Islambouli [45] and Akram et al. [2], which maximize the number of serviced users with minimum number of drones; Reina et al. [41], which focuses on maximizing the total user coverage; Cui et al. [12], where the coverage of indoor users and outdoor users are maximized while considering fairness; and Demiane et al. [14], in which the strategic waypoints are identified considering the heterogeneous importance levels of users, and the path among these points is optimized.

Among the reviewed studies that focus on damage assessment and relief distribution problems, Chowdhury et al. [8], Rabta et al. [40], Adsanver et al. [1] and Chowdhury et al. [9] consider recharging stations for drones in the network, whereas the others assume that the endurance of the drone is enough for conducting the operation and returning to the depot. Moreover, the en-route data transmission features are mentioned in Macias et al. [35], Bravo et al. [6], Reyes-Rubiano et al. [43], Ejaz et al. [16] and Worden et al. [48]; however, these features are not incorporated in the suggested formulations except for in Worden et al. [48], in which the authors focuses on a task assignment problem without the intermediary recharge possibilities. To the best of our knowledge, there exists no study that focuses on the routing problem of drones while considering the intermediary recharging stations and integrating the en-route remote data transmission in the proposed formulation simultaneously.

## ***2.2 Related Routing Problems***

The routing problem of drones holds similarities with the recharging electric vehicle routing problem (E-VRP) [44] or green vehicle routing problem (G-VRP) [18] in terms of battery endurance and charging limitations. Thus, the battery level-related constraints in the formulation suggested in this chapter are adapted from the E-VRP literature, specifically, from the notations proposed in Schneider et al. [44] and Froger et al. [21]. E-VRP is a widely studied area, where an extensive literature review can be found in Küçükoğlu et al. [30]. We provide examples from the literature which are closely related to our problem that considers previously located intermediary recharging stations.

Schneider et al. [44] introduce an E-VRP problem where they consider time windows and recharge stations. The vehicles are assumed to leave the recharge stations fully charged. The authors present a hybrid heuristic that combines a variable neighborhood search algorithm with a tabu search heuristic to solve the introduced problem. Keskin et al. [28] also focus on the electric vehicle routing problem with time windows while considering the time-dependent queueing times at the stations. An exact formulation is presented to solve small instances, where a combination of adaptive large neighborhood search and of the solution of a mixed integer linear program is developed for larger instances. Froger et al. [21] focus

on the nonlinear charging rate of vehicles, where the vehicles can be partially charged upon their visit to charging stations. An arc-based formulation is developed as an alternative to the classic node-based model, where the recharge stations are replicated as nodes, and a path-based formulation to avoid this replication that outperforms others. Bruglieri et al. [7] consider a setting where electric vehicles can partially recharge their batteries at the recharge stations and propose a three-phase metaheuristic that combines the exact method, variable search, and local branching. Andelmin and Bartolini [4] propose an exact algorithm to solve a path-based G-VRP modeled as a set partitioning problem. The authors apply dominating rules with valid inequalities to reduce the number of paths for an improved run-time.

As pointed out in Kūçūkođlu et al. [30], it is a basic assumption of E-VRP that each route starts and ends at the depot node, which is also the general assumption in the reviewed E-VRP literature. In the setting considered in this study, the UAVs do not need to return to the operation center to transmit the gathered information, thus, our problem is also related to the open vehicle routing problems (O-VRP). There is a vast amount of literature on O-VRP, which is reviewed in Li et al. [33]. Brandāo [5] proposes a tabu search algorithm developed for this problem and compares the performances with previously published heuristics, where Fleszar et al. [20] solve the problem with variable neighborhood search heuristic. Letchford et al. [32] develop a branch-and-cut algorithm considering the capacity limitations. The authors highlight the differences between the classical vehicle routing problem and the O-VRP modification and compare the results of these two notations. Allahviranloo et al. [3] focus on a selective version of the problem since it is more suitable in cases with uncertainty and limited resources. Three new formulations are proposed to undertake the uncertain demand levels. The DRP-RCOM, with recharging station features and the information transmission considerations, also contributes to the vehicle routing literature with new objectives motivated by a humanitarian context, such as expanding the coverage of assessment and decreasing the response time.

In summary, the use of drones in humanitarian operations is a growing literature; however, there is a gap in terms of incorporating the information transmission and battery recharge without the need to return to the operation center in the presented formulations. Our study contributes to the literature by introducing a novel mathematical formulation to the post-disaster assessment drone routing problem that considers the intermediary recharge stations and en-route information transmission in a partially available communication infrastructure network.

### 3 Problem Definition

In this study, we focus on assessing the damages in a disaster-affected area, which is represented by grids. Without loss of generality, we consider a post-earthquake setting since earthquakes cause significant damage to the built-in infrastructure, and the speed of assessment operations is critical to rescuing people that are stuck in

buildings. Each grid is given a priority score that represents the criticality level, whereas higher priority scores are given to more critical grids. The priority score of the grids may be assigned by disaster management authorities by considering different factors, such as the likelihood of damage, the importance of the buildings in the grid (e.g., schools, hospitals), and the density of the population.

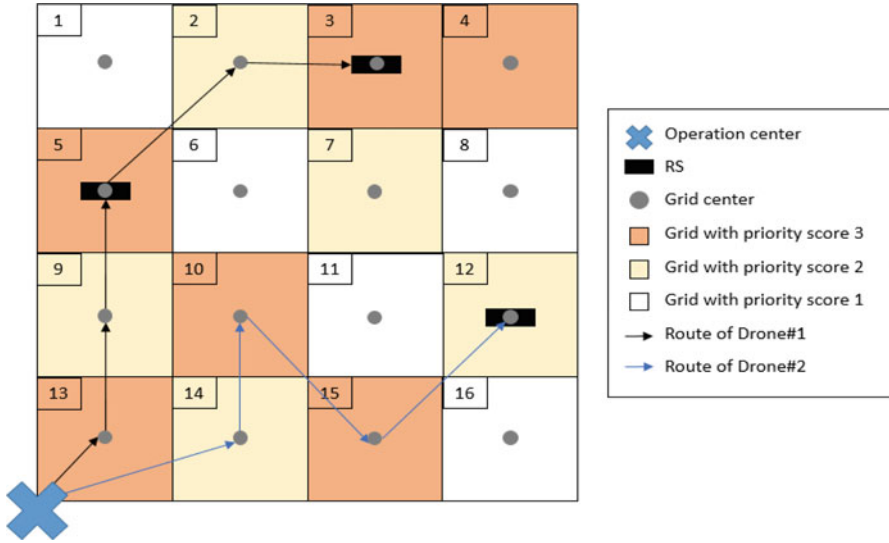
We aim to determine the routes of multiple identical drones completed within an assessment horizon so that the total priority scores obtained from the visited grids are maximized while reducing the response time for the assessed grids. We assume that the length of the assessment horizon, which specifies the maximum route duration for a drone, is decided a priori by the authorities based on the specific context. Moreover, we assume that in order to obtain information from a grid, the drone should spend a certain scanning time on that grid. The travel time between two grids is the time required to travel from the center of one grid to another.

We consider a homogeneous drone fleet with battery limitations and required hardware to record and transmit data. Drones are assumed to have sufficient storage capacity for recording and transmitting the footage obtained by grids during the assessment horizon. The battery limitation is an important aspect of the problem as the drones may not have enough battery to travel, scan, and transmit data within the assessment horizon. Thus, we consider RSs located in the center of certain grids in the grid network. One or more RS may be included in the routes of drones more than once, and the battery is assumed to be fully charged upon a visit to an RS. The charging time at RSs is determined by a linear battery charging rate. We assume that multiple drones can be charged at a single RS simultaneously.

We assume that there is a single operation center in this problem where the drones initially take off fully charged, and the information obtained from grids is processed and analyzed. Moreover, we assume an online setting, where the communication structure exists in the RS grids, and drones can transmit footage of the assessed grids to the operation center without the need to return to the center. During a route, a grid's footage is sent to the operation center at the next RS visit. This remote communication setting enables the decision-makers at the operation center to reach the necessary information regarding the situation of the area faster. We also take the data transmission features into account as follows. The necessary time to transmit the data is directly proportional to the amount of data to be transmitted, and the transmission rate is inversely proportional to the square of the distance between the operation center and the transmitting RS, due to the simplified path loss function [25], which results in required transmission time to increase proportionally to the squared distances.

Although all drones take off from the operation center at the beginning, there is no need for them to return to the operation center at the end of the assessment horizon since en-route footage transmission and recharge is possible. However, in order to send the information of all scanned grids to the operation center, all routes must end at an RS.

The aim is to visit as many grids as possible and transmit the collected information quickly, considering the criticality of the grids within the limited assessment horizon. Due to the remote communication structure that we consider



**Fig. 1** An exemplary solution of DRP-RCOM on a disaster-affected area divided into 16 grids

in this approach, we define this problem as the drone routing problem with remote communication (DRP-RCOM).

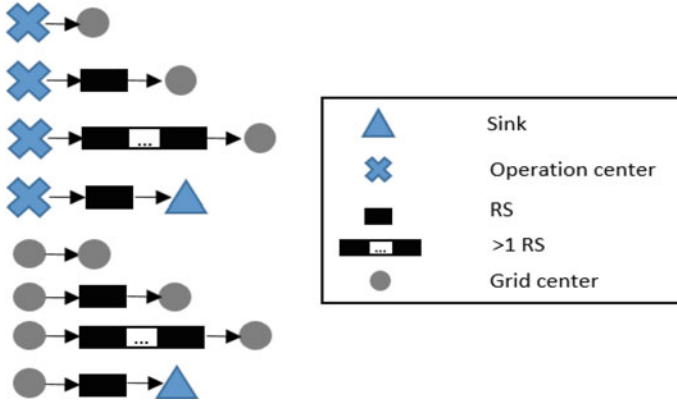
An exemplary network and the routes for DRP-RCOM are presented in Fig. 1. In this network, there are 16 grids, three RSs located at the center of grids #3, #5, and #12, and two drones. Initially, both drones start their route from the operation center. Drone#1 follows the route of grids #13, #9, #5, #5(RS), #2, #3, #3(RS). Note that the footage of grids #13, #9, and #5 are transmitted at #5(RS), whereas the footage of grids #2 and #3 are transmitted at #3(RS) at the end of the route. Similarly, Drone #2 follows the route of grids #14, #10, #15, #12, and #12(RS), where the footage of all grids is transmitted to the operation center at #12(RS) at the end of the route. We observe that both routes allowed the drones to scan the grids with higher priority scores.

We next present our mathematical model formulation for the DRP-RCOM.

### 3.1 Mathematical Model

We develop a path-based formulation for DRP-RCOM since it is shown to perform better than the arc-based formulation for the drone assessment routing problem [1]. In this approach, all possible paths are enumerated before the model is executed. All drones take off from the operation center, denoted as grid 0 in the formulation, at the beginning of the assessment horizon, and they follow routes consisting of one or more consecutive paths over the assessment horizon, as shown in Fig. 1. A path





**Fig. 2** Possible path structures

consists of a departure grid and an arrival grid, with zero or at least one RS grid in between, as illustrated in Fig. 2. Departure grids consist of the grids to be scanned and the origin grid, which is the operation center, whereas the arrival grids involve the grids to be scanned and the dummy sink node. All drone routes are ensured to end at an RS node so that all the information obtained from the scanned grids can be transmitted. The dummy sink node is used to ensure that all routes end at an RS grid. For this, we generate paths that start from a departure grid, visit the nearest RS grid, and end at the dummy sink node, and enforce each drone to take such a path at the end of their routes. We note that the travel times from the dummy sink node to all grids are considered to be equal to zero. All possible path structures are illustrated in Fig. 2.

We next present our formulation for the setting in which en-route transmission of data is performed in all visited RS grids. Afterward, we also explain how we adapt the proposed formulation to the setting where data transmission can only occur at the end of the route.

**Notation**

**Sets and Parameters**

- $\mathcal{I}$  set of grids to be scanned
- $\mathcal{V}_R$  set of RS grids
- $\mathcal{S}$  dummy sink node
- $\mathcal{V}$  set of nodes;  $\mathcal{V} = \mathcal{I} \cup \{0\} \cup \mathcal{V}_R \cup \{\mathcal{S}\}$
- $\mathcal{V}_0$  set of departure grids,  $\mathcal{V}_0 = \mathcal{I} \cup \{0\}$
- $\mathcal{V}_1$  set of arrival grids,  $\mathcal{V}_1 = \mathcal{I} \cup \{\mathcal{S}\}$
- $\mathcal{P}$  set of paths that originate from grids in  $\mathcal{V}_0$ , and ends at grids in  $\mathcal{V}_1$
- $\mathcal{P}_{ij}$  set of paths that connects grid  $i$  to grid  $j$ ,  $i \in \mathcal{V}_0, j \in \mathcal{V}_1$

$\mathcal{L}_p$	ordered set of RSs in path $p \in \mathcal{P}$
$o(p)$	starting grid of path $p \in \mathcal{P}$
$d(p)$	ending grid of path $p \in \mathcal{P}$
$s_j$	scanning time of grid (in minutes) $j \in \mathcal{I}$
$t_p$	travel time of path (in minutes) $p \in \mathcal{P}$
$t'_{ij}$	travel time from grid $i$ to grid $j$ , $i \in \mathcal{V}_0, j \in \mathcal{V}_1$
$\pi_{p(l)}$	RS at position $l \in \mathcal{L}_p$
$\alpha_{d(p)}$	closest RS to the ending grid of path $p \in \mathcal{P}$
$c_{p(l)}$	distance between the RS on path $p \in \mathcal{P}$ at $\pi_{p(l)}$ and the operation center
$\rho_j$	priority score of grid $j \in \mathcal{I}$
$B$	maximum battery capacity (in minutes)
$r$	time taken to recharge one unit (in minutes)
$T_{max}$	the route duration limit (assessment horizon) (in minutes)
$D$	number of drones
$e$	time taken to send one unit of information at RS (in minutes)
$w_1$	weight assigned to the first term of objective function, related to the total priority-weighted grid visits
$w_2$	weight assigned to the second term of objective function, related to the total untransmitted information amount before paths start
$M$	a very large number
$\epsilon$	a very small number

### Decision Variables

$x_p$	1 if a drone travels on path $p \in \mathcal{P}$ , and 0 otherwise.
$z_j$	1 if grid $j \in \mathcal{I}$ is visited by a drone, and 0 otherwise.
$a_p$	time before the drone starts traveling on path $p \in \mathcal{P}$ .
$y_p$	remaining battery level before the drone starts traveling on path $p \in \mathcal{P}$ .
$n_p$	untransmitted amount of stored footage obtained from grids before the drone starts traveling on path $p \in \mathcal{P}$ .
$q_{pl}$	remaining battery level after the drone travels on path $p \in \mathcal{P}$ and before visits $\pi_{p(l)}$ .

### Objective Function

The objective function of DRP-RCOM consists of three terms. The first term, denoted as  $O^{Ps}$ , maximizes the total priority scores obtained from the visited grids, as in (1).

$$O^{Ps} = \sum_{j \in \mathcal{I}} \rho_j z_j \quad (1)$$

The second term of the objective function minimizes the total amount of stored but untransmitted footage before the paths start, which is denoted as  $O^{Tr}$  and calculated as shown in (2).

$$O^{tr} = \sum_{p \in \mathcal{P}} n_p \quad (2)$$

The third term minimizes the flowtime, as shown in (3). However, this term only aims to eliminate alternative optima and is thus multiplied with a small coefficient in the objective function of DRP-RCOM.

$$O^{flow} = \sum_{p \in \mathcal{P}} a_p \quad (3)$$

The first and second terms are multiplied with importance weights in order to observe the trade-off in between. To eliminate the magnitude differences between the values of these two terms, they are scaled with respect to the maximum and the minimum possible values that can be obtained so that both terms take a value between 0 and 1. In order to scale the first two terms of the objective function, we calculate the minimum and maximum values of  $O^{ps}$  and  $O^{tr}$ , which are denoted as  $O_{min}^{ps}$ ,  $O_{max}^{ps}$ ,  $O_{min}^{tr}$ ,  $O_{max}^{tr}$ , respectively.

The minimum values for the first and second objectives,  $O_{min}^{ps}$  and  $O_{min}^{tr}$ , respectively, can be obtained without any calculations. That is, due to the constraints that ensure each path can be taken at most once (see (6)) and flow balance constraints (see (7)) in our formulation, one drone will take the path that travels from the depot to the nearest RS and then the dummy sink node, where other drones will visit a single grid to be scanned each, and then follow the path that travels to the nearest RS before the dummy sink node. In this case,  $D - 1$  grids will be visited. Thus,  $O_{min}^{ps}$  and  $O_{min}^{tr}$  will be equal to  $D - 1$ . However, calculating the maximum values for these objectives (i.e.,  $O_{max}^{ps}$  and  $O_{max}^{tr}$ ) is not as straightforward since there are many factors that need to be considered, such as the total route lengths, recharge limitations, and time requirements. To obtain upper bounds, the proposed formulation is solved with only the first and third terms of the objective function, as in (4).

$$\max \quad O^{ps} - \epsilon O^{flow} \quad (4)$$

This way, the total priority scores obtained from the visited grids and the amount of untransmitted stored footage will also be at their largest values since there is a time trade-off between visiting more grids and transmitting footage more frequently. The  $O_{max}^{ps}$  and  $O_{max}^{tr}$  values are then a posteriori calculated from the obtained solution.

The resulting combined objective function of DRP-RCOM is shown in (5).

$$\max \quad w_1 \left( \frac{O^{ps} - O_{min}^{ps}}{O_{max}^{ps} - O_{min}^{ps}} \right) - w_2 \left( \frac{O^{tr} - O_{min}^{tr}}{O_{max}^{tr} - O_{min}^{tr}} \right) - \epsilon O^{flow} \quad (5)$$

## Constraints

In this section, we introduce and explain the constraints of DRP-RCOM.

$$\text{s.t.} \quad \sum_{\substack{i \in V_0 \\ i \neq j}} \sum_{p \in P_{ij}} x_p \leq 1 \quad \forall j \in \mathcal{I}, \quad (6)$$

$$\sum_{\substack{i \in V_1 \\ i \neq j}} \sum_{p \in P_{ij}} x_p - \sum_{\substack{i \in V_0 \\ i \neq j}} \sum_{p \in P_{ji}} x_p = 0 \quad \forall i \in \mathcal{V}_1 \quad (7)$$

$$\sum_{j \in V_1} \sum_{p \in P_{0j}} x_p = D \quad (8)$$

$$\sum_{j \in V_0} \sum_{p \in P_{js}} x_p = D \quad (9)$$

$$\sum_{\substack{i \in V_0 \\ i \neq j}} \sum_{p \in P_{ij}} x_p = z_j \quad \forall j \in \mathcal{I} \quad (10)$$

$$\begin{aligned} \sum_{\substack{k \in V_1 \\ k \neq j}} \sum_{p \in P_{jk}} y_p &= \sum_{\substack{i \in V_0 \\ i \neq j}} \sum_{p \in P_{ij}} (y_p - (t_p + s_j)x_p \\ &+ \sum_{\substack{l \in \mathcal{L}_p \\ |\mathcal{L}_p| \neq 0}} (Bx_p - q_{pl})) \quad \forall j \in \mathcal{I} \end{aligned} \quad (11)$$

$$y_p - t'_{o(p), \pi_p(0)} x_p = q_{p0} \quad \forall p \in \mathcal{P} : |\mathcal{L}_p| \neq 0 \quad (12)$$

$$Bx_p - t'_{\pi_p(l-1), \pi_p(l)} x_p = q_{pl} \quad \forall p \in \mathcal{P} : |\mathcal{L}_p| \neq 0, l \in \mathcal{L}_p \setminus \{0\} \quad (13)$$

$$y_p = Bx_p \quad \forall i \in \mathcal{V}_1, p \in \mathcal{P}_{0i} \quad (14)$$

$$y_p \leq Bx_p \quad \forall p \in \mathcal{P} \quad (15)$$

$$q_{pl} \leq Bx_p \quad \forall p \in \mathcal{P}, l \in \mathcal{L}_p \quad (16)$$

$$y_p - (t_p + s_{d(p)})x_p + \sum_{l \in \mathcal{L}_p} (Bx_p - q_{pl}) - t'_{d(p), \alpha_{d(p)}} x_p \geq 0 \quad \forall p \in \mathcal{P} \quad (17)$$

$$\sum_{j \in V_1} \sum_{p \in P_{0j}} n_p = 0 \quad (18)$$

$$n_p \leq Mx_p \quad \forall p \in \mathcal{P} \quad (19)$$

$$\sum_{\substack{k \in V_1, \\ k \neq j}} \sum_{p \in P_{jk}} n_p = \sum_{\substack{i \in V_0, \\ i \neq j}} \sum_{p \in P_{ij}} (n_p + s_{d(p)}x_p - \sum_{\substack{l \in L_p, \\ |L_p| \neq 0}} n_p) \quad \forall j \in \mathcal{I} \quad (20)$$

$$\sum_{j \in V_1} \sum_{p \in P_{0j}} a_p = 0 \quad (21)$$

$$\begin{aligned} \sum_{\substack{k \in V_1, \\ k \neq j}} \sum_{p \in P_{jk}} a_p &= \sum_{\substack{i \in V_0, \\ i \neq j}} \sum_{p \in P_{ij}} (a_p + (t_p + s_j)x_p \\ &+ \sum_{\substack{l \in L_p, \\ |L_p| \neq 0}} (r(Bx_p - q_{pl}) + n_p c_l^2 e)) \quad \forall j \in \mathcal{I} \end{aligned} \quad (22)$$

$$a_p \leq T_{max} - (t_p - s_{d(p)})x_p - \sum_{\substack{l \in L_p, \\ |L_p| \neq 0}} (r(Bx_p - q_{pl}) + c_l^2 e n_p) \quad \forall p \in \mathcal{P} \quad (23)$$

$$a_p \leq Mx_p \quad \forall p \in \mathcal{P} \quad (24)$$

$$x_p \in \{0, 1\} \quad \forall p \in \mathcal{P} \quad (25)$$

$$a_p \geq 0, y_p \geq 0, n_p \geq 0 \quad \forall p \in \mathcal{P} \quad (26)$$

$$q_{pl} \geq 0 \quad \forall p \in \mathcal{P}, l \in \mathcal{L}_p \quad (27)$$

$$z_j \in \{0, 1\} \quad \forall j \in \mathcal{I} \quad (28)$$

Constraints (6) ensure that each path can be taken at most once. Constraints (7) are flow balance constraints for grids. Constraints (8) and (9) indicate that the number of taken paths that depart from the origin grid, and the paths whose arrival grid is the dummy sink node are equal to the number of available drones. Constraints (10) associate the visited paths with the visited grids. Constraints (11) track the drone's battery level at each grid. Constraints (12) determine the remaining battery level when the drone arrives at the first RS ( $\pi_{p(0)}$ ) on each path that consists of at least one RS, where constraints (13) track the battery level when the drone departs from an RS and arrives at the next RS for each path that contains more than one RS. Constraints (14) indicate the charge level at the origin grid at the beginning of the assessment horizon. Constraints (15) and (16) associate the battery level variables. Constraints (17) guarantee the path feasibility between a grid and the nearest RS, that is, the drone may arrive at the nearest RS without running out of battery. Constraints (18) and (19) ensure that the untransmitted stored footage amount is zero at the beginning of the assessment horizon and for the paths that the drones do not travel on. Constraints (20) define the untransmitted stored footage amount at the beginning of each path, where if an RS is visited, the stored amount is considered to be transmitted, and the newly scanned footage is added to the stored amount.

Constraints (21) define the starting time of the assessment operations. Constraints (22) determine the departure time from each grid, where the departure time from a grid is equal to the sum of the departure time from the previous grid, traveling time in between the grids, the scanning time of the current grid, total recharging time on the path, and the time required to transmit the stored footage from the visited RS grids. Since the data transmission occurs at the RSs, we assume that the battery limitations of the drones can be omitted since drones can recharge and transmit data simultaneously; however, the transmission increases the time spent at a path when it occurs. Constraints (23) ensures that the total route duration does not exceed the maximum route duration ( $T_{max}$ ). Constraints (24) guarantee that the time before the drones start traveling on a path is 0 if the drones do not travel on that path. Lastly, constraints (25)–(28) define the decision variables.

We also formulate a setting where no en-route transmissions are considered, and all stored data is transmitted at the last RS visited at the end of the route. We modify several constraints in the proposed formulation. Specifically, while determining the untransmitted stored footage amount in (20), we assume that the stored information is not transmitted in the intermediary RSs in this setting; thus, this constraint is modified as in (29).

$$\sum_{\substack{k \in \mathcal{V}_1, \\ k \neq j}} \sum_{p \in P_{jk}} n_p = \sum_{\substack{i \in \mathcal{V}_0, \\ i \neq j}} \sum_{p \in P_{ij}} (n_p + s_{d(p)} x_p) \quad \forall j \in \mathcal{I} \quad (29)$$

Moreover, the time required to transmit the data in the intermediary RSs is not considered anymore, and constraints (22) are modified to (30).

$$\sum_{\substack{k \in \mathcal{V}_1, \\ k \neq j}} \sum_{p \in P_{jk}} a_p = \sum_{\substack{i \in \mathcal{V}_0, \\ i \neq j}} \sum_{p \in P_{ij}} (a_p + (t_p + s_j) x_p + \sum_{\substack{l \in L_p, \\ |L_p| \neq 0}} r(Bx_p - q_{pl})) \quad \forall j \in \mathcal{I} \quad (30)$$

Finally, the time required for the data transmission is taken into account for the paths that arrive at the dummy sink node. For this adjustment, constraints (23) is adapted as (31).

$$a_p \leq T_{max} - (t_p - s_{d(p)}) x_p - \sum_{\substack{l \in L_p, \\ |L_p| \neq 0}} (r(Bx_p - q_{pl}) + c_l^2 e n_p) \quad (31)$$

$$\forall p \in \mathcal{P}_{ij}, i \in \mathcal{V}_0, j = \mathcal{S}$$

## 4 Numerical Analysis

In this section, we introduce our proposed performance metrics, illustrate the test instances, and discuss our findings on the results. We analyze the tradeoff between

the total priority scores obtained from the visited grids and the untransmitted data amount before the paths start. We also highlight the advantage of en-route transmission with the proposed performance metrics.

#### 4.1 Performance Metrics

We propose four performance metrics to assess the effectiveness of the drone routes as follows.

- **Percentage of unvisited grids** ( $m1$ ) represents the unvisited number of grids divided by the total number of grids in the given maximum route duration.
- **Priority-weighted percentage of unvisited grids** ( $m2$ ), which considers the priority of assessed grids, allows us to observe the importance of the unvisited grids in the network. The lower this metric is, especially compared to the percentage of unvisited grids, the better, since it means that the unvisited grids have low priorities.
- **Total response time** ( $m3$ ) indicates the sum of the time passed between the beginning of the routes and the time that the footage of the grid is transmitted. We assume that for the setting where en-route transmission occurs, all footage obtained and stored between two RS grids is sent at once upon any RS visit, whereas for the setting without en-route transmission, the response time of all grids is equal to each other, the total route duration. Lower values for this metric may occur under two circumstances; either the footage is transmitted frequently, resulting in a considerably low response time, especially for the grids assessed at the beginning of the interval, or fewer grids are visited.
- **Total priority-weighted response time** ( $m4$ ) is calculated as the summation of the priority score divided by the response time of each grid. High values indicate that the footage of more critical grids is transmitted faster.

In addition to these performance metrics, we also report the optimality gap and the runtime information while presenting results.

#### 4.2 Test Instances

We tested our model on small-sized randomly generated instances. The model is coded with Java and Concert Technology and solved on a computer with Intel Core i9-10980XE CPU 3.0 GHz and 128 GB of RAM. In all instances, the time required to charge the drones for one unit ( $r$ ) is assumed to be one minute, and a fully charged drone can operate for 60 minutes ( $B$ ). Travel times between grids ( $t_{ij}$ ) are calculated based on the Euclidean distance between the coordinates of the grid centers, and the speed of the drones is assumed to be constant. We assume that the scanning times ( $s_j$ ) for each grid are equal to 1 minute. The time required to transmit one unit of

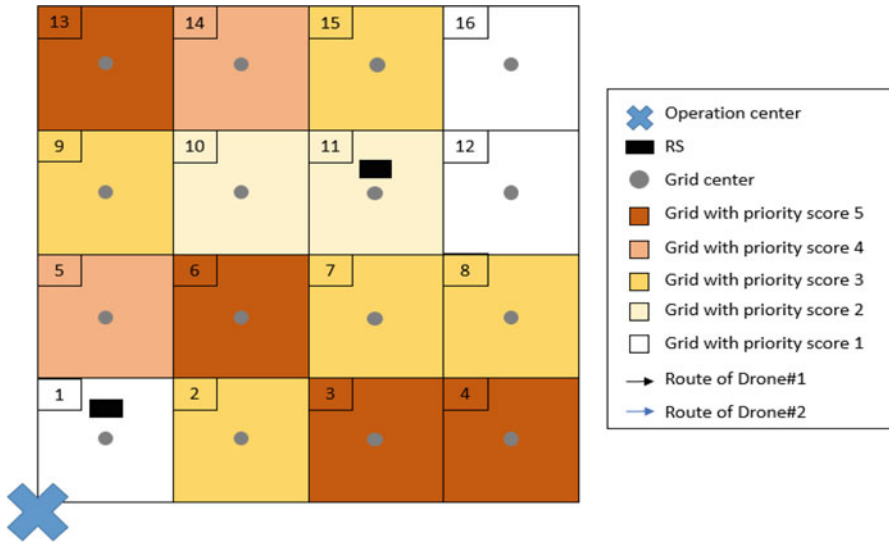


Fig. 3 Illustration of the test instance network

data ( $e$ ) is assumed to be 0.1 minutes. There exist two RS grids in the network, and on both RSs, the communication infrastructure is assumed to be established. We test the model on varying maximum route duration ( $T_{max}$ ) of 60, 90, and 120 minutes. The results were also compared for one, two, and three identical drones ( $D$ ) scanning the disaster-affected area.

The experiments were conducted on networks with 4, 9, 16, and 25 square grids with a side length of one kilometer and with varying priority scores between 1 and 5, where the most critical grid is represented with a priority score of 5. Presenting insights from the computational results is not possible when the network has few grids, such as four or nine grids, whereas a network with 25 grids is too large for the model to obtain results that are optimal or close to optimal. Thus, the analysis is performed on networks with 16 grids. We set a one-hour computational time limit for all instances.

Figure 3 illustrates the test instance network with 16 grids. Note that the RSs are assumed to be located in the center of the grids; however, in the figure, they are illustrated slightly distant from the grid center so that the visits to the grid centers and RSs can be differentiated.

### 4.3 Results

In this section, we first introduce a base instance where  $T_{max}$  is equal to 90 minutes,  $D$  is equal to 2, and the weights in the objective function  $w_1$  and  $w_2$  are equal



to 0.9 and 0.1, respectively. Then, we perform sensitivity analysis on  $w_1$  and  $w_2$  to observe the tradeoff between the total priority scores obtained from the visited grids and the untransmitted amount of information before each path starts. If higher importance is assigned to the total priority scores obtained from the visited grids, fewer visits to RSs occur since the travel time can be spent scanning more grids instead. Whereas if higher importance is assigned to the untransmitted amount of information before each path starts, more frequent visits to RS grids are expected to transmit the information, decreasing the amount of untransmitted information.

Moreover, we compare the numerical results with the case where the data transmission is only allowed at the RSs at the end of the routes. The aim of this comparison is to analyze the effect of en-route transmission on the number of visited grids and the response time. In the aftermath of a disaster, the communication infrastructure can be damaged, preventing the stored information from being transmitted from further points. In our approach, we propose a setting where the communication infrastructure is partially reconstructed or a temporary communication network is established only at the RS grids. The analysis in this section also highlights the importance of the re-established communication infrastructure, even if only for the RS grids.

Finally, we experiment under different  $D$  and  $T_{max}$  values in order to observe the effect of the number of drones operating over the disaster-affected area and the maximum route duration. Table 1 presents the parameter values and the results of our instances, including the value of four performance metrics  $m1$ ,  $m2$ ,  $m3$ , and  $m4$  introduced in Sect. 4.1, optimality gap, and runtime values.

First, we analyze the trade-off between the first two terms of the objective function that are the total priority scores obtained from the visited grids and the total amount of untransmitted footage before each path starts by varying  $w_1$  and  $w_2$  values in 0th, 1st, and 2nd instances in Table 1. The resulting routes for both drones are presented in Table 2. We observe that increasing the weight on the second term of the objective function related to the untransmitted footage amount results in a higher

**Table 1** Randomly generated small instance parameters and resulting performance metrics

Instance	En-Route Transm.	$w_1$	$w_2$	$D$	$T_{max}$ (min)	$m1$ (%)	$m2$ (%)	$m3$	$m4$	Gap (%)	Runtime (s)
0 (Base)	YES	0.9	0.1	2	90	0.0	0.0	3945.3	0.51	4.5	3604.8
1	YES	0.5	0.5	2	90	25.00	12.0	1594.5	0.51	17.2	3608.5
2	YES	0.1	0.9	2	90	93.8	90.0	68.6	0.07	0.0	1.2
3	NO	0.9	0.1	2	90	43.8	32.0	796.5	0.38	0.0	193.1
4	NO	0.5	0.5	2	90	56.3	38.0	616.1	0.35	0.0	37.8
5	NO	0.1	0.9	2	90	93.8	90.0	68.6	0.07	0.0	1.3
6	YES	0.9	0.1	2	60	0.0	0.0	5199.4	0.24	6.3	3601.5
7	YES	0.9	0.1	2	120	0.0	0.0	2888.8	0.54	3.1	3604.6
8	YES	0.9	0.1	1	90	37.5	24.0	3243.0	0.30	0.0	1627.1
9	YES	0.9	0.1	3	90	0.0	0.0	2317.2	0.7	1.8	3605.6

**Table 2** Routes of drones computed for instances 0, 1, and 2 to analyze different weight settings

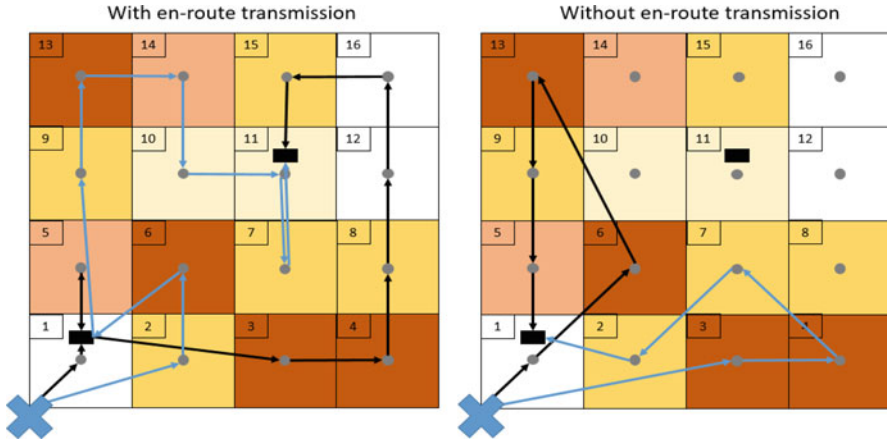
Instance	Drone #1 Route	Drone #2 Route
0	(Depot)0 - 1 - (RS)1 - 5 - (RS)1 - 3 - 4 - 8 - 12 - 16 - 15 - (RS)11 - Sink	(Depot)0 - 2 - 6 - (RS)1 - 9 - 13 - 14 - 10 - 11 - 7 - (RS)11 - Sink
1	(Depot)0 - 1 - (RS)1 - 9 - 5 - (RS)1 - 13 - 14 - 15 - (RS)11 - Sink	(Depot)0 - 2 - 7 - 6 - (RS)1 - 3 - 4 - 8 - (RS)11 - Sink
2	(Depot)0 - 6 - (RS)11 - Sink	(Depot)0 - (RS)1 - Sink

percentage and priority-weighted percentage of unvisited grids that are represented by metrics  $m1$  and  $m2$ , respectively. The reason for this increase is that decreasing the total untransmitted footage amount before each path starts can be achieved by reducing the obtained footage amount, thus, visiting fewer grids. For example, the results of the 2nd instance indicate that minimizing the total untransmitted footage amount before the paths start results in the minimum possible number of grids to be visited, as explained in detail in Sect. 3.1. According to the routes presented in Table 2, since there are two drones in the network, one of them travels through the nearest RS to the operation center and then the dummy sink node, where the other visits one critical grid and then transmits the footage on the nearest RS to that grid. In order to prevent fewer grids from being visited while decreasing the response time, a certain threshold for the minimum number of grids to be scanned can be imposed in the model.

As expected, metric  $m3$  in Table 1 shows that the total response time decreases as higher importance is assigned to the second term of the objective function; however, this is due to the fact that fewer grids are visited. The total priority-weighted response time metric  $m4$ , in which the response time is at the denominator, stays the same in the 1st instance and then decreases in the 2nd instance. The  $m4$  values for 0th and 1st instances show that although fewer grids are visited in the 1st instance, the critical grids are included in the routes, and their footage was transmitted earlier compared to the 0th instance. In addition, as shown in Table 2, the routes of drones in the 1st instance include fewer but critical grids in between RS visits and more frequent stops at RSs. Note that as we give equal weights to the first two parts of the objective, the model becomes more difficult to solve, and the optimality gap increases.

Next, we compare the results of two settings, where the obtained footage can be transmitted each time the drones visit an RS grid and where the transmission can be made only at the last visited RS. The results for these two settings are presented in Table 1 with instances 0, 1, 2, 3, 4, and 5. We observe that when en-route transmissions are allowed, the percentage and the priority-weighted percentage of unvisited grids (metrics  $m1$  and  $m2$ ) decreases for instances 0 and 1 compared to instances 3 and 4. The 2nd and 5th instances yield the same results since the weight setting causes the minimum possible amount of grids to be visited. The resulting routes from instances 0 and 3 are illustrated in Fig. 4 for the test instance.

Figure 4 shows that in the case where en-route transmission is allowed all grids can be visited within  $T_{max}$ . Moreover, the drones visit RS grids multiple times



**Fig. 4** The routes of drones where en-route transmission is allowed (Instance 0) vs. not allowed (Instance 3)

during their routes to transmit footage and recharge. We observe that the last visited RS grid is further away from the operation center; thus, the drones have ray-shaped routes. The reason for this structure is the intermediary transmissions in the closer RS grids and less amount of footage to be transmitted from RSs that are further away. This structure also allows more grids to be visited since the travel time required to return to the RS grid that is closer to the operation center can be spent scanning more grids. All grids are visited by drones when the en-route transmission is possible, whereas 43.75% of the grids cannot be visited when the en-route transmission is not possible, as depicted in Fig. 4. Without the en-route transmission, the routes are constructed in a way to cover the critical grids that are closer to the operation center, as observed from the values of metrics  $m_2$ ,  $m_3$ , and  $m_4$  in Table 1 and Fig. 4. This is due to the fact that the time required to transmit data depends on the distance from the operation center, and although returning to the depot is not necessary for DRP-RCOM, we observe that the routes end by an RS grid that is close to the operation center and form a petal shape to minimize the required amount of time for transmission. That is, we observe a trade-off between the travel time to the closest RS grid and the time required to transmit data from RS grids that are further from the operation center.

Similar results were obtained for the 1st and 4th instances, where en-route transmissions allow more grids to be visited than the case with no en-route transmissions. However, in order to decrease the total amount of untransmitted information in this weight setting, fewer grids are visited in both communication settings compared to instances 0 and 3. We also observe from Table 1 that the runtimes for this setting are considerably low, and all instances could be solved at optimality since the RS grids are solely visited for recharge purposes, and the time required to transmit data is not taken into account for the routing decisions except the last transmitting RS in the case without the en-route transmission.

Next, we experiment on different  $T_{max}$  values for the given network with the 0th, 6th, and 7th instances. We observe from Table 1 that for each given value to  $T_{max}$  (i.e., 60, 90, 120), all grids in the network can be visited. However, there exists a decrease for the total response time metric  $m3$  and an increase for the priority-weighted total response time metric  $m4$  as  $T_{max}$  value increases. Since all grids are visited for all three instances, the increase in metric  $m4$  indicates that the footage of scanned grids is transmitted to the operation center earlier as the maximum route duration increases. Thus, we can infer that the routes of the drones are constructed in a way that more intermediary RS grids are included when the route duration is longer. Note that the further the RS is from the operation center, the longer time (proportional to the squared distance) is needed to transmit the data, as shown in constraints (22) and (23). We observe that increasing the total route duration has a positive effect on decreasing the response time.

Finally, the effects of the number of drones can be assessed from the solutions of instances 8 and 9. From Table 1, we observe that with a single drone, 37.5% of the grids cannot be visited; however, the critical grids are included in the route of the drone, as the priority-weighted percentage of unvisited grids, metric  $m2$ , is less than the percentage of unvisited grids (metric  $m1$ ). Although metric  $m3$  has decreased for the 8th instance compared with 0th, this is due to fewer grids visited. Another indicator of the decreased number of visited grids for the 8th instance is the total priority-weighted response time (metric  $m4$ ).

With two and three drones, all grids can be scanned within the assessment horizon. Metrics  $m3$  and  $m4$  presented in Table 1 indicate that using more drones is beneficial in terms of the response time to grids, as with three drones, more frequent visits to RSs are possible.

With the obtained results, we observe that decreasing the untransmitted footage amount at the beginning of each path results in visiting fewer grids. Moreover, the results show the positive impact of partially available communication infrastructure and en-route remote data transmission on the number of visited grids, and the response time. We finally discuss the benefit of increasing the number of drones and maximum route duration with the proposed performance metrics.

## 5 Conclusion

This study aims to support the response operations by determining routes for drones in order to systematically assess the damage levels in the disaster-affected area. We consider an online setting where the obtained information is transmitted to the operation center without the need to return. This approach brings the advantages of decreasing the response times for the assessed grids, and obtaining information from more grids in the case where the time for assessment operations is limited. Moreover, we consider intermediary recharge stations in the routes of drones, so that the limited battery endurance is handled. We divide the affected area into grids and prioritize the critical grids using priority scores. We consider multiple drones assessing the area.

We develop a mathematical model that incorporates a number of essential factors that must be accounted for using drones in a post-disaster assessment environment. The proposed model aims to maximize the total priority scores obtained from the visited grids and transmit the information earlier in the route. We also minimize the flowtime with a small penalty to eliminate alternative optima. To measure and be able to compare the performance of the model under different settings, we propose four performance metrics that are mainly based on the number of visited grids and the response time. We present the behavior of our model under different parameter settings on a set of small-sized instances. We show the effect of the value of the weights in the objective function, where we present a trade-off between the total priority scores obtained from the visited grids and the response time. Moreover, we show the advantage of considering en-route transmission of the information to the operation center rather than transmitting all the information at the end of the route, both for the total priority scores obtained from the visited grids and the response time. Finally, we comment on the changes in the proposed metrics as we experiment with different maximum route duration and number of drone values.

Since post-disaster drone routing is an emerging topic in the literature, there can be many interesting extensions to the presented work. First, due to the complexity of the presented model, only trivial-sized instances could be solved to optimality for validation purposes. Therefore, an effective practical heuristic algorithm would be necessary for solving realistic larger-sized instances quickly. Varying charging rates and effect of different movements of the drones, such as escalating, declining, or rotation activities on the battery consumption, are possible extensions of this work. Finally, considering different possibilities for the availability of communication infrastructure and information transmission frequency (e.g., transmitting data after scanning each grid) can be addressed in future research.

**Acknowledgments** This work was supported by the Scientific and Technical Research Council of Turkey under Scientific and Technological Research Projects Funding Program (1001 TUBITAK) grant with agreement number 121M857.

## References

1. Adsanver, B., Çoban, E., Balçık, B.: Drone routing for post-disaster damage assessment. In: Kotsireas, I.S., Nagurney, A., Pardalos, P.M., Tsokas, A. (eds.) *Dynamics of Disasters*. Springer Optimization and Its Applications 169, chapter 1, pp. 1–29. Springer, Switzerland AG (2021)
2. Akram, T., Awais, M., Naqvi, R., Ahmed, A., Naeem, M.: Multicriteria uav base stations placement for disaster management. *IEEE Syst. J.* **14**, 3475–3482 (2020)
3. Allahviranloo, M., Chow, J.Y., Recker, W.W.: Selective vehicle routing problems under uncertainty without recourse. *Transport. Res. Part E* **62**, 68–88 (2014)
4. Andelmin, J., Bartolini, E.: An exact algorithm for the green vehicle routing problem. *Transport. Sci.* **51**, 1031–1386 (2017)
5. Brandão, J.: A tabu search algorithm for the open vehicle routing problem. *Eur. J. Oper. Res.* **157**, 552–564 (2004)

6. Bravo, R.Z.B., Leiras, A., Oliveira, F.L.C.: The use of UAVs in humanitarian relief: An application of POMDP-based methodology for finding victims. *Prod. Oper. Manag.* **28**, 421–440 (2019)
7. Bruglieri, M., Mancini, S., Pezzella, F., Pisacane, O., Suraci, S.: A three-phase matheuristic for the time-effective electric vehicle routing problem with partial recharges. *Electron. Notes Discrete Math.* **58**, 95–102 (2017). 4th International Conference on Variable Neighborhood Search
8. Chowdhury, S., Emelogu, A., Marufuzzaman, M., Nurre, S.G.: Drones for disaster response and relief operations: a continuous approximation model. *Int J. Prod. Econ.* **188**, 167–184 (2017)
9. Chowdhury, S., Shahvari, O., Marufuzzaman, M., Li, X.: Drone routing and optimization for post-disaster inspection. *Comput. Ind. Eng.* **159**, 107495 (2021)
10. Countinho, W.P., Fliege, J., Battara, M.: Glider routing and trajectory optimisation in disaster assessment. *Eur. J. Oper. Res.* **274**, 1138–1154 (2019)
11. CRED and UNDRR (2020). The human cost of disasters: an overview of the last 20 years (2000–2019). <https://www.undrr.org/publication/human-cost-disasters-overview-last-20-years-2000-2019>. Accessed 28 May 2022
12. Cui, J., Hu, B., Chen, S.: A decision-making scheme for UAV maximizes coverage of emergency indoor and outdoor users. *Ad Hoc Netw.* **112**, 102391 (2021)
13. Daud, S.M.S.M., Yusuf, M.Y.P.M., Heo, C.C., Khoo, L.S., Singh, M. K.C., Mahmood, M.S., Nawawi, H.: Applications of drone in disaster management: a scoping review. *Sci. Justice* **62**, 30–42 (2022)
14. Demiane, F., Sharafeddine, S., Farhat, O.: An optimized UAV trajectory planning for localization in disaster scenarios. *Comput. Netw.* **179**, 107378 (2020)
15. DJI, Enterprise: Croatian mountain rescue service—using drones for earthquake response in Petrinja (2021). <https://enterprise-insights.dji.com/user-stories/drone-earthquake-response-croatia-petrinja>. Accessed 31 May 2022
16. Ejaz, W., Ahmed, A., Mushtaq, A., Ibnkahla, M.: Energy-efficient task scheduling and physiological assessment in disaster management using UAV-assisted networks. *Comput. Commun.* **155**, 150–157 (2020)
17. Erdelj, M., Król, M., Natalizio, E.: Wireless sensor networks and multi-UAV systems for natural disaster management. *Comput. Netw.* **124**, 72–86 (2017)
18. Erdoğan, S., Elise, M.-H.: A green vehicle routing problem. *Transport. Res. Part E: Logist. Transport. Rev.* **48**(1), 100–114 (2012)
19. Fikar, C., Gronalt, M., Hirsch, P.: A decision support system for coordinated disaster relief distribution. *Expert Syst. Appl.* **57**, 104–116 (2016)
20. Fleszar, K., Osman, I.H., Hindi, K.S.: A variable neighbourhood search algorithm for the open vehicle routing problem. *Eur. J. Oper. Res.* **195**, 803–809 (2009)
21. Froger, A., Mendoza, J.E., Jabali, O., Laporte, G.: Improved formulations and algorithmic components for the electric vehicle routing problem with nonlinear charging functions. *Comput. Oper. Res.* **104**, 256–294 (2019)
22. FSD: Drones in humanitarian action—a guide to the use of airborne systems in humanitarian crises (2016). <https://reliefweb.int/report/world/drones-humanitarian-action-guide-use-airborne-systems-humanitarian-crises>. Accessed 31 May 2022
23. Gabbert, B.: Drones photograph the damage in paradise caused by the camp fire (2018). <https://wildfiretoday.com/2018/11/24/drones-photograph-the-damage-in-paradise-caused-by-the-camp-fire/>. Accessed 30 May 2022
24. Golabi, M., Shavarani, S.M., Izbrak, G.: An edge-based stochastic facility location problem in UAV-supported humanitarian relief logistics: a case study of Tehran earthquake. *Nat. Hazards* **87**, 1545–1565 (2017)
25. Goldsmith, A.: *Wireless Communications*. Cambridge University Press, Cambridge (2005)
26. Grogan, S., Pellerin, R., Gamache, M.: Using tornado-related weather data to route unmanned aerial vehicles to locate damage and victims. *OR Spectr.* **43**, 905–939 (2021)

27. IFRC: Emergency needs assessments (2022). <https://www.ifrc.org/emergency-needs-assessments>. Accessed 28 May 2022
28. Keskin, M., Laporte, G., Çatay, B.: Electric vehicle routing problem with time-dependent waiting times at recharging stations. *Comput. Oper. Res.* **107**, 77–94 (2019)
29. Khaled, Z.E., Mcheick, H.: Case studies of communications systems during harsh environments: a review of approaches, weaknesses, and limitations to improve quality of service. *Int. J. Distrib. Sensor Netw.* **15**(2), 1550147719829960 (2019)
30. Küçükoglu, I., Dewil, R., Cattrysse, D.: The electric vehicle routing problem and its variations: a literature review. *Comput. Ind. Eng.* **161**, 107650 (2021)
31. Kyriakakis, N.A., Marinaki, M., Matsatsinis, N., Marinakis, Y.: A cumulative unmanned aerial vehicle routing problem approach for humanitarian coverage path planning. *Eur. J. Oper. Res.* **300**, 922–1004 (2022)
32. Letchford, A., Lysgaard, J., Eglese, R.: A branch-and-cut algorithm for the capacitated open vehicle routing problem. *J. Oper. Res. Soc.* **58**, 1642–1651 (2007)
33. Li, F., Golden, B., Wasil, E.: The open vehicle routing problem: algorithms, large-scale test problems, and computational results. *Comput. Oper. Res.* **34**, 2918–2930 (2007)
34. Luege, T.: Case study no. 12: Using drones in fire and rescue services in the United Kingdom (2016). <https://europa.eu/capacity4dev/innov-aid/discussions/case-study-no-12-using-drones-fire-and-rescue-services-united-kingdom>. Accessed 31 May 2022
35. Macias, J.E., Goldbeck, N., Hsu, P.-Y., Angeloudis, P., Ochieng, W.: Endogenous stochastic optimisation for relief distribution assisted with unmanned aerial vehicles. *OR Spectr.* **42**, 1089–1125 (2020)
36. Macrina, G., Pugliese, L.D.P., Guerriero, F., Laporte, G.: Drone-aided routing: a literature review. *Transport. Res. C* **120**, 102762 (2020)
37. Oruç, B.E., Kara, B.Y.: Post-disaster assessment routing problem. *Transport. Res. B* **116**, 76–102 (2018)
38. Palliyaguru, R., Amaratunga, D., Haigh, R.: Effects of post disaster infrastructure reconstruction on disaster management cycle and challenges confronted: the case of Indian ocean tsunami in Sri Lanka. In: *The 7th International Postgraduate Research Conference*. The University of Salford, Salford (2007)
39. PrecisionHawk: A history of drones in hurricane response (2019). <https://www.precisionhawk.com/blog/a-history-of-drones-in-hurricane-response>. Accessed 30 May 2022
40. Rabta, B., Wankmüller, C., Reiner, G.: A drone fleet model for last-mile distribution in disaster relief operations. *Int. J. Disaster Risk Reduct.* **28**, 107–112 (2018)
41. Reina, D., Camp, T., Munjal, A., Toral, S.: Evolutionary deployment and local search-based movements of 0th responders in disaster scenarios. *Fut. Gener. Comput. Syst.* **88**, 61–78 (2018)
42. Rejeb, A., Rejeb, K., Simske, S., Treiblmaier, H.: Humanitarian drones: a review and research agenda. *Internet of Things* **16**, 100434 (2021)
43. Reyes-Rubiano, L., Voegl, J., Rest, K.-D., Faulin, J., Hirsch, P.: Exploration of a disrupted road network after a disaster with an online routing algorithm. *OR Spectr.* **43**, 289–326 (2021)
44. Schneider, M., Stenger, A., Goeke, D.: The electric vehicle-routing problem with time windows and recharging stations. *Transport. Sci.* **48**, 500–520 (2014)
45. Sharafeddine, S., Islambouli, R.: On-demand deployment of multiple aerial base stations for traffic offloading and network recovery. *Comput. Netw.* **156**, 52–61 (2019)
46. Stumpf, J., Guerrero-Garcia, S., Lamarche, J.-B., Besiou, M., Rafter, S.: Supply chain expenditure and preparedness investment opportunities (2017). <https://www.actioncontrelaifaim.org/en/publication/supply-chain-expenditure-preparedness-investment-opportunities-in-the-humanitarian-context/>. Accessed 15 July 2022
47. Townsend, A., Moss, M.: Telecommunications infrastructures in disasters: preparing cities for crisis communications (2005). <https://sarwiki.informatik.hu-berlin.de/images/2/2a/Report1.pdf>. Accessed 15 July 2022
48. Worden, M.R., Murray, C.C., Karwan, M.H., Ortiz-Peña, H.J.: Sensor tasking for unmanned aerial vehicles in disaster management missions with limited communications bandwidth. *Comput. Ind. Eng.* **149**, 106754 (2020)

49. Zhu, M., Du, X., Zhang, X., Luo, H., Wang, G.: Multi-UAV rapid-assessment task-assignment problem in a post-earthquake scenario. *IEEE Access* **7**, 74542–74557 (2019)
50. Zorn, C.R., Shamseldin, A.Y.: Post-disaster infrastructure restoration: a comparison of events for future planning. *Int. J. Disaster Risk Reduct.* **13**, 158–166 (2015)



# Identifying Critical Nodes in a Network



Ashwin Arulsevan and Altannar Chinchuluun

## 1 Introduction

Many network applications require the elements of their network in working condition in order to guarantee the overall operation of the network. However, not all elements of the network contribute equally to the operational efficiency. From this standpoint, it is imperative to identify the nodes that contribute to the operations of the network. We refer to [8, 12] that treats the subject of quantifying operational efficiency of various network applications with respect to its topological properties. For the purposes of this chapter, we present our problems and methods with respect to network fragmentation and cohesion. Both these terms are quite loose and vague, but we will make them more precise as we introduce the problems and motivate them through concrete applications. Much of the problems and methods discussed in this chapter will be introduced as a combinatorial problem and discrete optimization techniques will be used to solve them in a deterministic setting. A lot of developments have happened in the last decade, and techniques based on simulation, heuristics, machine learning algorithms, and uncertainty modeling have been developed. For a full overview of these topics, we refer the reader to [13, 18, 22]. An alternative way of looking at these problems would be as

---

A. Arulsevan (✉)

Department of Management Science, Strathclyde Business School, Glasgow, Scotland, UK  
e-mail: [ashwin.arulsevan@strath.ac.uk](mailto:ashwin.arulsevan@strath.ac.uk)

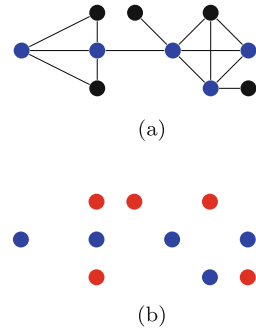
A. Chinchuluun

Department of Finance, Business School, National University of Mongolia, Ulaanbaatar, Mongolia

Institute of Mathematics and Digital Technology, Mongolian Academy of Sciences, Ulaanbaatar, Mongolia

e-mail: [altannar@num.edu.mn](mailto:altannar@num.edu.mn)

**Fig. 1** Vertex cover and independent set problem. **(a)**  $k$ -vertex cover. **(b)**  $(|V| - k)$ -Independent set



generalizations of well-known graph theory problems. Most classical graph theory problems involve requiring us to identify a set of nodes or edges to be deleted or included in a graph, so the resulting graph would satisfy some requirement. However, one must be aware that there is no unique way to generalize these problems. In the maximum clique problem (MCP) [7], we are given an undirected graph  $G(V, E)$  and we seek the largest subgraph that is complete. A generalization of this is to seek a graph that is as dense as possible given we can pick at most  $k$  nodes. This is the densest  $k$ -subgraph problem (DkS) that was introduced in [14]. There are numerous other generalizations such as  $k$ -cliques,  $k$ -plex,  $k$ -clubs, etc. (see [5]). In an independent set problem (ISP), we are given an undirected graph  $G(V, E)$  and we seek to find the largest subgraph that is empty. In other words, we are interested in finding the largest subgraph that is empty or the smallest set of nodes to be deleted that results in an empty graph. A similar generalization, as the DkS for Clique, would be to seek a set of  $k$  nodes to be deleted that maximizes pairwise disconnectivity. We call this the critical node detection problem (CNDP), [3]. In a vertex cover problem (VCP), we are given an undirected graph and seek the smallest set of nodes such that every edge in the graph has at least one end point in the graph. An alternative way of looking at this is by minimizing the set of nodes deleted such that the resultant subgraph is empty (see Fig. 1).

A set of vertices that has at least one endpoint of every edge is called a vertex cover. A minimum vertex cover is the complement of the maximum independent set of the graph. A natural extension of the vertex cover problem, as we extended the ISP to CNDP, would be the cardinality-constrained critical node detection problem (CC-CNDP). This was introduced in [4], where we are interested in determining the minimum set of nodes to be deleted, so that the size of the largest component in the remaining graph is bounded by an input integer  $L$ . Although VCP and ISP are equivalent in the optimization sense, they are not equivalent in the approximation preserving sense. Independent set problem has no constant factor [6] approximation and Vertex cover problem has a two-factor approximation [21]. This kind of result also exists for the CNDP and CC-CNDP. We will look at these complexity results in the subsequent sections. As we mentioned earlier, various other generalizations are possible for all these problems. We are interested in the exposition of these three generalizations in this chapter.

## 1.1 Applications of the Problems

All these problems have many direct applications in the real world. In addition to being viewed as generalizations of classical graph theory problems, these can be motivated through these applications. We mention some of them here. In covert networks, we are interested in suppressing or jamming communications. One can identify critical nodes to place jammers in case of a communication network, and in case of social network, we can think of these networks as individuals who need to be significantly influenced to prevent propagation of information. In social networks, particularly in contagion of epidemic in contact networks, we are interested in identifying individuals who should be targeted for immunization in order to have maximum control over the spread of a pathogen. In drug design, protein networks are analyzed to identify proteins that are present in multiple pathways. In emergency response, we are interested in identifying shelter locations in order to minimize the distance of nodes from the located shelters. In case of social networks, in addition to identifying nodes that are responsible for propagation of information, we are also interested in identifying dense clusters that represent a homogeneous group of individuals with similar interests.

## 2 Critical Node Detection Problem

The critical node detection problem was introduced in [3]. Given an undirected graph  $G(V, E)$  and an integer  $k$ , the critical node detection problem seeks a subset of node  $S \subset V$ , with  $|S| \leq k$ , whose deletion results in maximum pairwise disconnectivity (or minimum pairwise connectivity). This problem can be formulated as follows:

$$\min \sum_{i \in V} \sum_{j \in V: i \neq j} x_{ij} \quad (1)$$

$$x_{ij} + y_i + y_j \geq 1 \quad \forall (i, j) \in E \quad (2)$$

$$x_{ij} + x_{jk} + x_{ik} \neq 2 \quad \forall (i, j, k) \in V \times V \times V \quad (3)$$

$$\sum_{i \in V} y_i \leq k \quad (4)$$

$$\mathbf{x} \in \{0, 1\}^{n^2} \quad (5)$$

$$\mathbf{y} \in \{0, 1\}^n \quad (6)$$

In the above program, the binary variables  $y_i$  take a value 1 if node  $i \in V$  is deleted and 0 otherwise. Binary variables  $x_{ij}$  take the value 1 if  $i$  and  $j$  are connected in the node-deleted subgraph. Constraint set (2) models the requirement that for every

edge  $(i, j) \in E$  in the graph, either node  $i$  or node  $j$  must be deleted or the pair of nodes  $i$  and  $j$  must be connected. Constraint set (3) models the requirement that no two pairs of nodes from the triple  $\{i, j, k\}$  can be connected if the third pair of the triple is disconnected. The “ $\neq$ ” constraint is modeled as a set of three constraints for every triple  $\{i, j, k\}$ :

$$\begin{aligned} x_{ij} + x_{jk} - x_{ik} &\leq 1 \\ x_{ij} - x_{jk} + x_{ik} &\leq 1 \\ -x_{ij} + x_{jk} + x_{ik} &\leq 1 \end{aligned}$$

Constraint set (4) model the requirement that at most  $k$  nodes can be deleted. Constraint sets (5)–(6) model the binary requirement of the decision variables. The objective function (1) simply counts the number of pairs of nodes that are disconnected from each other. The correctness of the above formulation has been discussed in [3]. The work also proposed a heuristic where maximal independent sets were randomly sampled and the complement set gets deleted. If the complement set is less than  $k$ , then it gets augmented in a greedy fashion. The final set is further improved with a local search. The maximal independent set sampling algorithm was applied to a wide variety of computer-generated and real-world instances. The relaxation of the formulation given in (1)–(6) has an unbounded gap. Tightening of the formulation using valid inequalities is still open. There is an alternative perspective to the objective function of CNDP. We are given a subset of nodes,  $S \subseteq V$ , whose deletion from  $G$  results in  $M$  connected components in the node-deleted subgraph  $G[S]$ . Let  $\sigma_h$  be the size of component  $h$  of  $G[S]$ . An algebraic representation of the pairwise connectivity in terms of the connected components in  $G[S]$  is

$$\sum_{h \in M} \frac{\sigma_h(\sigma_h - 1)}{2}$$

Based on this, the following lemma was provided to characterize the properties of the objective function of the CNDP in [3].

**Lemma** *Let  $M$  be a partition of  $G = (V, E)$  into  $L$  components obtained by deleting a set  $D$  of nodes, where  $|D| = k$ . Then the objective function  $\sum_{h \in M} \frac{\sigma_h(\sigma_h - 1)}{2} \geq \frac{(|V| - k)^2}{2(L - 1)}$ , with equality holding if and only if  $\sigma_h = \sigma_l, \forall h, l \in M$ , where  $\sigma_h$  is the size of  $h^{th}$  component of  $M$ .*

This lemma indicates that when we have  $|M|$  components in the graph, the best possible objective value can be attained if all components are of equal size.

**Lemma** *Let  $M_1$  and  $M_2$  be two sets of partitions obtained by deleting  $D_1$  and  $D_2$  sets of nodes, respectively, from graph  $G = (V, E)$ , where  $|D_1| = |D_2| = k$ . Let  $L_1$  and  $L_2$  be the number components in  $M_1$  and  $M_2$ , respectively, and  $L_1 \geq L_2$ .*

If  $\sigma_h = \sigma_l, \forall h, l \in M_1$ , then we obtain a better objective function value by deleting the set  $D1$ .

This lemma indicates that among two solutions both resulting in an equal component size upon deletion, the solution with the most number of components provides the best objective value. The intuition behind both this lemma in characterization is that the objective function is seeking nodes to delete that results in maximum fragmentation of the graph. From an application perspective, we want to have as many clusters (or components) of nodes as possible and at the same time we do not want the individual clusters to be of disproportionate size from one another.

In addition, the problem was shown to be NP-complete. A simpler reduction could be given through a reduction from the decision version of the independent set problem, wherein we are given a graph  $G(V, E)$  and we are interested in knowing if there is a subset of vertices  $S$  with  $|S| \geq K$  such that the node induced subgraph  $G[S]$  is empty. The critical node detection problem on the same graph with input  $k = |V| - K$  will have an objective value of 0 if and only if the corresponding instance of independent set problem has a YES solution and a value of at least 1 otherwise. This reduction also provides the hardness of approximation hardness for CNDP for general graphs. For optimization, it does not matter whether we study CNDP as a maximization or a minimization problem, but this becomes relevant when we are interested in designing approximation algorithm. As we are interested in studying CNDP as a generalization of ISP, we take the objective to be maximization of the graph's disconnectivity.

**Definition** For a maximization problem, an algorithm is  $\alpha$ -approximate if it terminates with a solution with a value  $\geq \alpha$  OPT, where OPT is the optimal value.

The following result about approximation hardness is well known [28].

**Lemma** Let  $A$  be an NP-hard problem and there is a polynomial time reduction  $A \leq_P B$  such that for each instance  $I$  of  $A$ , the corresponding instance  $I'$  of  $B$

- Returns a value of at most  $\alpha$  if  $I$  is a YES instance
- Returns a value at least  $\beta$  if  $I$  is a NO instance

We cannot have  $\frac{\beta}{\alpha}$  approximation algorithm for problem  $B$

From the above lemma, we have that CNDP cannot be approximated unless  $P=NP$ . Unlike the independent set problem that has approximation guarantees for graph families like the planar and degree-bounded graphs, we do not have such guarantees for CNDP for special graph families if the independent set problem is NP-complete for those families. In fact, the problem is a lot harder as it has been shown in [11] that CNDP is NP-complete in trees when we consider general cost coefficients in the objective function. However, the weighted independent set problem on trees can be solved in linear time. On the positive side, there is a polynomial time algorithm for CNDP for trees with unit weights on nodes and unit cost coefficients [11]. An enumerative dynamic program was provided to solve the general case that runs in  $O(1.618^n)$  time.

We define a fixed-parameter-tractable problem as follows.

**Definition** Given a parameter  $k$  as an input and size of the input is  $n$ , is there an algorithm to an NP-complete problem that runs in  $f(k)O(n^c)$ , where  $f(k)$  is a function (possibly exponential) in  $k$ .

Unfortunately, through a reduction from clique cover problem CNDP was proved to be not fixed-parameter-tractable [10] either.

## 2.1 Further Research

As we have seen, CNDP is hard to approximate just as ISP from a worst-case perspective even for special graph families. Randomized greedy algorithms have been proposed for the independent set problem [17] that provide good bounds. Results in similar flavor or results that rule out such possibilities would be of interest. With the advances in data science, learning methods have been developed recently [13] to solve these problems with a number of interesting open questions. In addition, we do not have too many polyhedral results and valid inequalities proposed for the integer program proposed or any alternate formulations.

## 3 Cardinality-Constrained Critical Node Detection Problem

A cardinality-constrained node detection problem takes an undirected graph  $G(V, E)$  and an integer  $L$  as input and it seeks to minimize the number of nodes deleted such that the remaining node-deleted subgraph has no component of size greater than  $L$ . In terms of a mixed integer formulation, a minor adjustment to (1)–(6) would result in

$$\max \sum_{i \in V} y_i \tag{7}$$

$$x_{ij} + y_i + y_j \geq 1 \quad \forall (i, j) \in E \tag{8}$$

$$x_{ij} + x_{jk} + x_{ik} \neq 2 \quad \forall (i, j, k) \in V \times V \times V \tag{9}$$

$$\sum_{i \in V} x_{ij} \leq L - 1, \quad \forall j \neq i \tag{10}$$

$$\mathbf{x} \in \{0, 1\}^{n^2} \tag{11}$$

$$\mathbf{y} \in \{0, 1\}^n \tag{12}$$

The constraints (8) and (9) perform the same function as in CNDP. Objective function (7) simply minimizes the total number of nodes deleted and constraint (10)

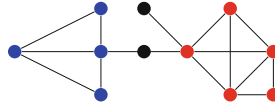
restricts the number of nodes connected to any single node by  $L - 1$ . This in turn restricts the size of the largest component by  $L$ . Note that this problem falls under the more general category of node deletion problems proposed in [20]. In node deletion problems, we are given an undirected graph and are interested in minimizing the number of nodes deleted such that the node-deleted subgraph satisfies a certain property. Examples of these properties include planarity, empty subgraph, and bounded degree. The properties, however, need to be hereditary, which means that if a graph satisfies the property then any subgraph must also satisfy the property. From an optimization perspective, if a node-deleted subgraph satisfies this property, deleting more nodes will not result in violation of the property. The second condition for the property is that it has to be nontrivial, that is, it should hold true for an infinite family of graphs. It is not difficult to see that CC-CNP is a node deletion problem and our property that the largest component of node-deleted subgraph has to be of size at most  $L$  is both hereditary and nontrivial. [19] has shown both NP-hardness and Max-SNP hardness of these problems. On the positive side, we note that this problem is similar to set cover problem that can be observed through an alternate formulation. Just as the case in CNDP, the above formulation has an unbounded gap. An alternative formulation would be in terms of the set cover problem, wherein we have a better formulation:

$$\begin{aligned} & \min \sum_{i \in V} x_i \\ & \sum_{i \in S} x_i \geq 1, \quad \forall S \subset V, |S| = L + 1, G[S] \text{ is connected} \\ & \mathbf{x} \in \{0, 1\}^{|V|} \end{aligned}$$

The above corresponds to a set cover formulation. We can get  $\min(O(L), O(\log n))$ -approximation using the LP relaxation [28] of the set cover based formulation. Note that formulation has exponentially many constraints. However, separation boils down to finding the largest component in a graph, which can be done in  $O(|V|)$  time using a depth-first search. In terms of the hardness, one can only state one cannot approximate the problem within a factor of  $2 - \epsilon$  from the results of vertex cover problem [15]. It is not clear whether the approximation hardness results of set cover problem can be carried over to CC-CNP.

From a heuristic perspective, the independent set sampling heuristic can be adapted to solve this problem [4]. However, pathological instances can be created, and in addition, the authors have provided a genetic algorithm that significantly outperforms the MIS-based heuristic.

One of the open questions for this problem is that we do not whether fixed-parameter-tractable algorithm that runs in  $f(k, L)O(n^c)$  is possible for CC-CNP.



**Fig. 2** Densest subgraph problem. The nodes inducing the densest subgraphs corresponding to  $k = 4$  (blue) and  $k = 5$  (red) are given

### 4 Densest k-Subgraph Problem

In the densest  $k$ -subgraph problem (DkS), we are given an undirected graph  $G(V, E)$  and an integer  $k$ . We are interested in finding a set of  $k$  nodes, which induces the densest subgraph, that is, the number of edges in the induced subgraph is maximized (Fig. 2).

The problem was introduced in [14] and was shown as NP-hard even when the maximum degree is less than or equal to 3. The problem is also APX-hard in general. The best-known approximation in the general case is  $O(n)$ . For the bounded degree graphs with degree less than  $d$ , a few more results are known for the densest  $k$ -subgraph problem (DkS-d) [2]:

#### 4.1 Hardness of DkS-d

- APX-hard assuming the small set expansion (SSE) conjecture is true
- $(1 - e^{-\frac{1}{d}})$ -approximation is possible ( $\approx \frac{1}{d}$ )

Given  $d$ -regular graph  $G(V, E)$ , expansion of a subset  $S \subset V$  is defined by

$$\Phi_G(S) := \frac{|E(S, V \setminus S)|}{d|S|},$$

Now we define the expansion of the graph with respect to  $\delta > 0$  as

$$\Phi_G(\delta) := \min_{|S|=\delta|V|} \Phi_G(S).$$

We define the Gap-SSE problem as follows:

**Definition (Gap-SSE  $(\eta, \delta)$ )** Given a  $d$ -regular graph  $G(V, E)$  and constants  $\eta, \delta > 0$  distinguish whether

- Yes:  $\Phi_G(\delta) \leq \eta$   
 No:  $\Phi_G(\delta) \geq 1 - \eta$

The SSE conjecture is stated as follows:



**Conjecture ([23])** For every  $\eta > 0$ , there exist a  $\delta$  such that Gap-SSE  $(\eta, \delta)$  problem is NP-hard.

**Theorem ([2])** The DkS-d is APX-hard.

We outline the proof here. First, an intermediate problem is set up where one is interested in finding a set  $S$  of  $k$  nodes that has the maximum value for  $\frac{2|E(S)|}{dk}$ . Next note that this intermediate problem is equivalent to DkS. Let  $\bar{\Phi}_G(\delta) := 1 - \Phi_G(\delta)$ . This would distinguish instances

Yes:  $\bar{\Phi}_G(\delta) \geq 1 - \eta$  and  
 No:  $\bar{\Phi}_G(\delta) \leq \eta$ .

Assuming that the SSE conjecture is true, this would yield a contradiction.

### 4.2 Algorithms for DkS-d

The algorithms discussed here also work when there are weights on nodes  $w : V \rightarrow \mathbb{R}_+$  and profits on edges  $p : E \rightarrow \mathbb{R}_+$ . In this case, one wants to pick nodes whose weights are within a budget  $B$  given as input. The DkS problem has unit weights and profits with a budget of  $k$ . The algorithms can also be applied to hypergraphs (where an edge can correspond to more than two nodes). For an edge  $e \in E$ , we denote  $N(e)$  as the set of nodes corresponding to that edge. For a simple graph  $|N(e)| = 2$ . We define weights on edges based on the set of nodes corresponding to them. Define  $w'_e := \sum_{i \in N(e)} \frac{w_i}{d_i}$ , where  $d_i$  is the degree of node  $i$ . Note that we are interested in a  $d$ -degree-bounded graph and the largest degree  $\max_{i \in V} d_i = d$ . We first provide a weak algorithm to DkS-d and write the mixed integer program for this problem:

$$\begin{aligned} \mathcal{P}_1 : \max & \sum_{e \in E} p_e x_e \\ & \sum_{i \in V} w_i y_i \leq B \\ & y_i \geq x_e, \quad \forall e \in E, i \in N(e) \\ & \mathbf{y} \in \{0, 1\}^{|V|} \\ & \mathbf{x} \in \{0, 1\}^{|E|} \end{aligned}$$

In the above formulation,  $x_e$  is a variable corresponding to edge  $e$ , indicating if it is picked in the optimal solution or not. Consider a formulation

$$\mathcal{P}_2 : \max \sum_{e \in E} w_e x_e$$

$$\sum_{e \in E} w'_e x_e \leq \frac{B}{d}$$

$$\mathbf{y} \in \{0, 1\}^{|V|}$$

Note that every integral feasible solution to  $\mathcal{P}_2$  is feasible to  $\mathcal{P}_1$ . Also, every feasible solution to  $\mathcal{P}_1$  scaled down by  $d$  is feasible to  $\mathcal{P}_1$ . So  $\frac{1}{\alpha}$ -approximation to  $\mathcal{P}_2$  immediately gives a  $\frac{1}{d\alpha}$ -approximation to  $\mathcal{P}_1$ .  $\mathcal{P}_2$  is a knapsack problem that has a FPTAS. So one could get a  $\frac{1}{d+\epsilon}$ -approximation to DkS-d. However, a greedy algorithm with a tighter analysis would give a better approximation. A description of the greedy algorithm is given below:

1. Arrange edges by profit to weight ratio  $\frac{p_e}{(\sum_{i \in N(e)} w'_i)}$
2. Enumerate all edge sets of size  $\leq 2$
3. Augment the set with edges in the above order (until budget  $B$  is not violated)

Note that the greedy algorithm is the same as the one given by [16, 24, 29]. With a tighter analysis, one can show that

**Theorem ([2])** *The greedy algorithm results in  $(1 - e^{-\frac{1}{d}})$ -approximation for DkS-d.*

## 5 Distance-Based Critical Node Detection Problem

The distance-based critical node detection problem (DCNDP) was introduced and studied in [25] as a generalization of CNDP and but can also be perceived as a generalization of classic graph theory problems. In a DCNDP, we are given an undirected graph  $G(V, E)$  and an input integer  $k$ . We seek a subset of nodes  $S \subset V$  with  $|S| \leq k$  to be deleted such that the sum of pairwise distances of the nodes is minimized. We predominantly focus on the following two classes of distance functions defined on a pair of nodes  $i$  and  $j$ :

**Class 1** Minimize the number of node pairs connected by a path of length at most  $L$ , where  $L$  is an input

$$f_1(d_{ij}) = \begin{cases} 1, & \text{if } d_{ij} \leq L \\ 0, & \text{if } d_{ij} > L \end{cases} \tag{13}$$

$d_{ij}$  is the shortest distance between nodes  $i$  and  $j$  in the node-deleted subgraph  $G[V \setminus S]$  and  $L$  is a given positive integer representing the cut-off distance. The case where  $L \geq |V| - 1$  when we have unit weights on edges is the CNDP that we studied earlier where we simply minimize the number of connected node pairs.

**Class 2** Minimize the Harary index or efficiency of the graph

$$f_2(d_{ij}) = \begin{cases} d_{ij}^{-1}, & \text{if } d_{ij} < \infty \\ 0, & \text{if } d_{ij} = \infty \end{cases}$$

$d_{ij}$  is the shortest distance between nodes  $i$  and  $j$ . This is based on the assumption in networks that operational efficiency between node pairs is inversely proportional to the distance between them [9]. We assume disconnected nodes are at a distance of  $\infty$ . This corresponds to the fragmentation objective of CNDP. In [27], the authors introduced a threshold model, where two nodes separated by some distance threshold,  $L$ , cannot communicate directly, resulting in the following modified Harary distance function.

$$f_3(d_{ij}) = \begin{cases} d_{ij}^{-1}, & \text{if } d_{ij} \leq L \\ 0, & \text{otherwise} \end{cases} \tag{14}$$

A compact mixed integer formulation was given [26] and computational results were provided. An exponential-sized formulation was given in [1] which was tightened further using cutting planes.

### 5.1 Compact MIP Formulations

We can assume WLOG that  $G$  is connected. If this is not the case, we simply have to apply our algorithms to the individual components. We first have a binary decision variable  $x_i$  for each node  $i$  that takes a value 1 if node  $i$  is deleted and 0 otherwise. We then have the connectivity variables

$$y_{ij}^l = \begin{cases} 1, & \text{if } (i, j) \text{ are connected by a path of length } \leq l \text{ in } G^R \\ 0, & \text{otherwise.} \end{cases} \tag{15}$$

The following compact model was provided in [27].

$$y_{ij}^1 + x_i + x_j \geq 1, \quad \forall (i, j) \in E, i < j \tag{16}$$

$$y_{ij}^l + x_i \leq 1, \quad \forall (i, j) \in V, i < j, l \in \{1, 2, \dots, L\} \tag{17}$$

$$y_{ij}^l + x_j \leq 1, \quad \forall (i, j) \in V, i < j, l \in \{1, 2, \dots, L\} \tag{18}$$

$$y_{ij}^l = y_{ij}^1, \quad \forall (i, j) \in E, i < j, l \in \{2, \dots, L\} \tag{19}$$

$$y_{ij}^l \leq \sum_{t \in i} y_{ij}^{l-1}, \quad \forall (i, j) \notin E, i < j, l \in \{2, \dots, L\} \tag{20}$$

$$y_{ij}^l \geq y_{ij}^{l-1} - x_i, \quad \forall (i, t) \in E, (i, j) \notin E, i < j, l \in \{2, \dots, L\} \tag{21}$$

$$\sum_{i \in V} x_i \leq k \tag{22}$$

$$y_{ij}^l \in \{0, 1\}, \quad \forall (i, j) \in V, i < j, l \in \{1, \dots, L\} \tag{23}$$

$$x_i \in \{0, 1\}, \quad \forall i \in V \tag{24}$$

Constraints (16) ensure that  $y_{ij}^1 = 1$  if there is an edge between  $i$  and  $j$  and neither of the nodes  $i$  and  $j$  are deleted. Constraints (17)–(18) enforce  $y_{ij}^l$  to be zero if either node  $i$  or  $j$  is deleted. These constraints are not required but provide a tighter formulation. Constraints (20)–(21) force the binary variable  $y_{ij}^l$  to take a value 1 between two non-adjacent nodes  $i$  and  $j$  if and only if node  $i$  is not deleted and there exists a path of length  $l - 1$  between node  $t$  and node  $j$  for some immediate neighbor  $t$  of  $i$ . We denote the set of neighbors of node  $i$  as  $N(i)$ . Constraint (22) limits the number of nodes to be deleted to  $k$ . Constraints (23)–(24) enforces the binary restrictions. The binary restriction on the  $y$  variables can be relaxed without losing integrality in the optimal solution.

In [27], they noted that for all node pairs  $i$  and  $j$  with the shortest path distance  $d_{ij} > l$  we can set  $y_{ij}^l = 0$  and constraints (20)–(21) have to be defined only for  $l \geq d_{ij}$ . In addition, only the neighbours  $t \in N(i)$  with the shortest path  $d_{ij} \leq l - 1$  have to be considered in constraints (20)–(21). These preprocessing steps significantly reduce the number of variables and constraints in the model. The set of possible solutions to the DCNDP is then given by the set

$$\mathcal{P} := \{x \in \{0, 1\}^n, y \in \{0, 1\}^{m \times L} : (x, y) \text{ satisfies (16) to (24)}\}$$

Note that we only need to change the objective function if the distance class changes. The MIP model corresponding to the distance function (13) will be

$$\min_{(x,y) \in \mathcal{P}} \sum_{i,j \in V: i < j} y_{ij}^L \tag{25}$$

Objective (25) minimizes the number of node pairs whose shortest path distance is at most  $L$ . Similarly, the MIP model corresponding to distance connectivity metric (14) will be:

$$\min_{(x,y) \in \mathcal{P}} \sum_{i,j \in V: i < j} \left( f_3(1)y_{ij}^1 + \sum_{l=2}^L f_3(l) (y_{ij}^l - y_{ij}^{l-1}) \right) \tag{26}$$

Note that the objective function (26) computes the sum of the inverse of distances of all pairs of nodes. We assume the distance past the threshold ( $L$ ) as  $\infty$ . Note that this MIP model is not technically compact. If we do not consider hop distances, then we have pseudopolynomially many variables. An alternative formulation was given in [1] that has exponentially many constraints but polynomial number of

variables regardless of the distance. This exploits the structure of the first distance objective (13). Since we only need to consider paths of length at most  $L$ , by keeping track of paths within this threshold, we can guarantee that any given node pair  $(i, j)$  is  $L$ -distance disconnected if and only if at least one node along every path within a distance  $L$  between  $i$  and  $j$  is deleted. This avoids using the  $l$ - index in the distance connectivity variable  $y_{ij}^l$ , and has polynomially many variables. The path-based model has exponentially many constraints as each constraint corresponds to a path and there can be exponentially many of them. However, these can be separated very efficiently in practice. The connectivity variable  $y_{ij}$  is defined for every node pair  $i$  and  $j$ . It takes a value of 1 if nodes  $i$  and  $j$  are connected by a path of distance at most  $L$  and 0 otherwise. The same node deletion decision variables  $\mathbf{x}$  will be used along with the new connectivity variables  $\mathbf{y}$ . For a path  $P$ , we denote  $V(P)$  as the set of nodes in the path and  $\mathcal{P}(i, j)$  as the set of all paths between nodes  $i$  and  $j$ . The path-based model for distance objective function (13) is formulated as follows:

$$\text{minimize} \quad \sum_{i,j \in V: i < j} y_{ij} \tag{27}$$

$$\text{s.t.} \quad \sum_{r \in V(P)} x_r + y_{ij} \geq 1, \quad \forall P \in \mathcal{P}(i, j), |P| \leq L, (i, j) \in V, i < j \tag{28}$$

$$\sum_{i \in V} x_i \leq k \tag{29}$$

$$y_{ij} \in \{0, 1\}, \quad \forall (i, j) \in V, i < j \tag{30}$$

$$x_i \in \{0, 1\}, \quad \forall i \in V \tag{31}$$

Objective function (27) minimizes the number of node pairs that are connected by a path of distance at most  $L$ . Constraint (28) ensures that for every path of length at most  $L$  between node pairs  $(i, j)$  at least one node is deleted or node  $i$  and  $j$  are connected. Constraint (29) restricts the number of nodes that can be deleted to  $k$ . Constraints (30)–(30) enforce binary restrictions. The integrality constraint on the connectivity variables can be relaxed as they will be integers at optimality. The straightforward extension of the path-based formulation for the second distance function, class (14), does not avoid the use of pseudopolynomially many  $\mathbf{y}$  variables. It is as follows.

$$\text{minimize} \quad \sum_{i,j \in V: i < j} \left( f_3(1)y_{ij}^1 + \sum_{l=2}^L f_3(l) \left( y_{ij}^l - y_{ij}^{l-1} \right) \right) \tag{32}$$

$$\text{s.t.} \quad \sum_{r \in V(P)} x_r + y_{ij}^{|P|} \geq 1, \quad \forall P \in \mathcal{P}(i, j), |P| \leq L, i, j \in V, i < j \tag{33}$$

$$\sum_{i \in V} x_i \leq k \quad (34)$$

$$y_{ij}^l \in \{0, 1\}, \quad \forall (i, j) \in V, \quad i < j, \quad i \neq j, \quad l \in \{1, \dots, L_2\} \quad (35)$$

$$x_i \in \{0, 1\}, \quad \forall i \in V \quad (36)$$

The constraints are similar to those of the previous model. Like in all previous cases, the binary restriction on the connectivity variable  $\mathbf{y}$  does not have to be imposed. One could aggregate the connectivity variables and treat them as a continuous variable, that is,  $y_{ij}$  is a continuous variable that denotes the distance between nodes  $i$  and  $j$ . This gives us a modified formulation that has polynomial many variables (see [1] for a complete description). However, such an aggregated model would result in a poor primal bound. In [1], the formulations were further tightened using cuts that were based on odd holes present in the network. An efficient separation heuristic was provided based on depth-first trees constructed from the linear relaxation values.

Much of the investigation on other distance classes and heuristic and machine learning-based computational studies can be explored.

## 6 Conclusions

In this work, we explored four different critical node identification problems that could be either perceived as generalizations of classic graph theory problems or be motivated directly through their applications. We looked at their definitions, characterizations, and computational complexity. We also discussed some exact, approximate, and heuristic algorithms to solve them. We finally provided some open lines of investigation for these problems.

## References

1. Alozie, G.U., Arulsevan, A., Akartunali, K., Pasilio Jr., E.L.: Efficient methods for the distance-based critical node detection problem in complex networks. *Comput. Oper. Res.* **31**, 105254 (2021)
2. Arulsevan, A.: A note on the set union knapsack problem. *Discrete Appl. Math.* **169**, 214–218 (2014)
3. Arulsevan, A., Commander, C.W., Elefteriadou, L., Pardalos, P.M.: Detecting critical nodes in sparse graphs. *Comput. Oper. Res.* **36**(7), 2193–2200 (2009)
4. Arulsevan, A., Commander, C.W., Shylo, O., Pardalos, P.M.: Cardinality-constrained critical node detection problem. In: *Performance Models and Risk Management in Communications Systems*, pp. 79–91. Springer, Berlin (2011)
5. Balasundaram, B., Butenko, S. and Hicks, I.V.: Clique relaxations in social network analysis: the maximum k-plex problem. *Oper. Res.* **59**(1), 133–142 (2011)

6. Bazgan, C., Escoffier, B., Paschos, V.T.: Completeness in standard and differential approximation classes: poly-(D)APX- and (D)ptas-completeness. *Theor. Comput. Sci.* **339**(2–3), 272–292 (2005)
7. Bomze, I.M., Budinich, M., Pelillo, M., Pardalos, P.M.: Handbook of Combinatorial Optimization, chapter The maximum Clique Problem, pp. 1–74. Kluwer Academic Publishers, Norwell (1999)
8. Borgatti, S.P., Everett, M.G.: A graph-theoretic perspective on centrality. *Soc. Netw.* **28**(4), 466–484 (2006)
9. Crucitti, P., Latora, V., Marchiori, M., Rapisarda, A.: Efficiency of scale-free networks: error and attack tolerance. *Phys. A: Stat. Mech. Appl.* **320**, 622–642 (2003)
10. Hermelin, D., Kaspí, M., Komusiewicz, C., Navon, B.: Parameterized complexity of critical node cuts. *Theoret. Comput. Sci.* **651**(2016), 62–75 (2016)
11. Di Summa, M., Grosso, A., Locatelli, M.: Complexity of the critical node problem over trees. *Comput. Oper. Res.* **38**(12), 1766–1774 (2011)
12. Ellens, W., Kooij, R.E.: Graph Measures and Network Robustness (2013)
13. Fan, C., Zeng, L., Sun, Y., Liu, Y.-Y.: Finding key players in complex networks through deep reinforcement learning. *Nat. Mach. Intell.* **1**, 317–324 (2020)
14. Feige, U., Peleg, D., Kortsarz, G.: The densest  $k$ -subgraph problem. *Algorithmica* **29**, 410–421 (2001)
15. Khot, S., Regev, O.: Vertex cover might be hard to approximate to within  $2\epsilon$ . *J. Comput. Syst. Sci.* **74**(3), 335–349 (2008)
16. Khuller, S., Moss, A., Naor, J.: The budgeted maximum coverage problem. *Inform. Process. Lett.* **70**, 39–45 (1999)
17. Krivelevich, M., Mészáros, T., Michaeli, P., Shikhelman, C.: Greedy maximal independent sets via local limits. In: Drmota, M., Heuberger, C. (eds.) 31st International Conference on Probabilistic, Combinatorial and Asymptotic Methods for the Analysis of Algorithms (AofA 2020), volume 159 of Leibniz International Proceedings in Informatics (LIPIcs), pp. 20:1–20:19, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik
18. Lalou, M., Tahraoui, M.A. and Kheddouci, H.: The critical node detection problem in networks: a survey. *Comput. Sci. Rev.* **28**, 92–117 (2018)
19. Lund, C., Yannakakis, M.: The approximation of maximum subgraph problems. In: International Colloquium on Automata, Languages, and Programming ICALP 1993: Automata, Languages and Programming, pp. 40–51 (1983)
20. Lewis, J.M., Yannakakis, M.: The node-deletion problem for hereditary properties is np-complete. *J. Comput. Syst. Sci.* **20**(2), 219–230 (1980)
21. Papadimitriou, C.H., Steiglitz, K.: Combinatorial Optimization: Algorithms and Complexity. Prentice Hall India (1981)
22. Pullan, W.: Heuristic identification of critical nodes in sparse real-world graphs. *J. Heuristics* **21**, 577–598 (2015)
23. Raghavendra, P., Steurer, D.: Graph expansion and the unique games conjecture. In: STOC, pp. 755–764 (2010)
24. Sviridenko, M.: A note on maximizing a submodular set function subject to a knapsack constraint. *Oper. Res. Lett.* **32**(1), 41–43 (2004)
25. Veremyev, A., Boginski, V., Pasiliao, E.L.: Exact identification of critical nodes in sparse networks via new compact formulations. *Optim. Lett.* **8**(4), 1245–1259 (2014)
26. Veremyev, A., Prokopyev, O.A., Pasiliao, E.L.: An integer programming framework for critical elements detection in graphs. *J. Comb. Optim.* **28**(1), 233–273 (2014)
27. Veremyev, A., Prokopyev, O.A., Pasiliao, E.L.: Critical nodes for distance-based connectivity and related problems in graphs. *Networks* **66**(3), 170–195 (2015)
28. Williamson, D., Shmoys, D.: Design of Approximation Algorithms. Cambridge University Press, Cambridge (2010)
29. Wolsey, L.A.: Maximising real-valued submodular functions: primal and dual heuristics for location problems. *Math. Oper. Res.* **7**, 410–425 (1982)

# Machine Learning-Based Rumor Controlling



Ke Su, Priyanshi Garg, Weili Wu, and Ding-Zhu Du

## 1 Introduction

As the world enters the era of Web2.0, social media, such as Facebook, Twitter, and Weibo, have undergone rapid development in recent decades and have already become an inseparable part of our lives. According to the survey from Pew Research, the proportion of online social media adult users in all American adult population was 5% in 2007 and has grown to 65% in 2015 [57]. In the world, billions of people are connected by social media.

The content on traditional media, such as television, radio, and newspapers, is created by professionals and verified before being published to an audience or readers. On social media, every user is eligible to publish content, and the fact-checking mechanism is absent. Every day, tons of messages, images, and videos are posted to social media without verification. Due to connectivity, information spreads rapidly over social media, including rumors.

For example, starting in 2019, the world entered a pandemic period with the outbreak of the new crown epidemic. At the same time, various widespread COVID-19 rumors appeared on social media. For instance, someone linked the 5G network to COVID-19 [40]. One version of this rumor claimed that all news reports about COVID-19 were an elaborate scam, and the 5G network was the real reason that led to the COVID-19 symptom. Another version was that the 5G network could weaken the immune system, making people susceptible to viruses, according to an analysis by the *New York Times* [62]. On Facebook, the COVID-19/5G rumor communities attracted half a million followers in just two weeks. The rumor was

---

K. Su · P. Garg, W. Wu · D.-Z. Du (✉)

Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA

e-mail: [kxs130330@utdallas.edu](mailto:kxs130330@utdallas.edu); [priyanshi.garg@utdallas.edu](mailto:priyanshi.garg@utdallas.edu); [weiliwu@utdallas.edu](mailto:weiliwu@utdallas.edu); [dzdu@utdallas.edu](mailto:dzdu@utdallas.edu)



found in more than 30 countries. The COVID-19/5G rumor fueled people's panic. During the pandemic period, multiple cities reported that the 5G tower was attacked, and telecommute technicians were harassed. The COVID-19/5G rumor caused not only significant economic losses but also affected public security.

Intensive efforts have been made to control rumors [17, 18]. However, it is hard to analyze social network data due to its size, noise, and dynamism [59]. Machine learning, a technology that aims to enable autonomous learning based on a large volume of data to find out hidden patterns and make predictions, could be an effective solution. Machine learning significantly reduces human intervention compared to traditional expert systems based on rules. However, machine learning-based solutions still rely on carefully crafted features (feature engineering). Deep learning, the most popular machine learning branch, goes one step further. It can capture optimal features and discover indirect relations between features and goals. Research shows deep learning models can achieve the same level of accuracy without feature engineering [30]. Among all kinds of deep learning algorithms, it is worth mentioning graph neural network (GNN), which has attracted the research community's attention in recent years. GNN works on graph data. Therefore, they naturally fit the social media data. GNN can capture the structure of the social network, which is the pain point of other machine learning models that are not designed for graph data.

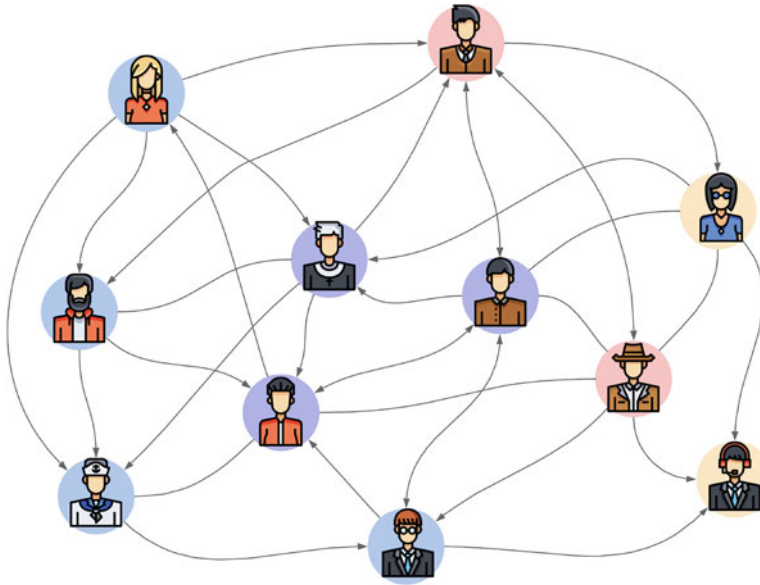
The structure of this chapter is as follows. Section 2 covers the related concepts, which are the graph model of OSN and the definition of rumor. Section 3 explains basic machine learning algorithms, including conventional machine learning models and neural network models. Section 4 shows features that could be used for social rumor research. Section 5 reviews the machine learning-based solutions for rumor detection, rumor source detection, and rumor prevention, which are three aspects of rumor control approaches. Section 6 is the conclusion. In each section, existing research efforts are reviewed and possible potential research problems are explored.

## 2 Related Concepts

### 2.1 Online Social Network

Online social network (OSN) is a virtual social network that consists of online users and the relations between them. OSN usually is modeled as a graph  $G = (V, E)$ , where  $V = \{v_1, v_2, \dots, v_{|V|}\}$  representation all nodes, and  $E \subseteq V \times V$  represents all edges.  $e_{ij} \in E$  means there is an edge between nodes  $v_i$  and  $v_j$ . The graph could be directed or undirected, depending on the intrinsic characteristics of the OSN. Pallavicini et al. [56] divided the relations between users into two types (Fig. 1):

- “Two way”: Represented by an undirected graph, a typical social platform is Facebook. Friends on Facebook are all following each other. Connected users can



**Fig. 1** Online social network example

exchange private messages and check each other's profiles and recent activities. Friends form a closed social network, and members know each other.

- “Star”: Represented by a directed graph. A typical social platform is Twitter. The sender and receiver of information are not equal, and they do not know each other.

Each social network is associated with an information diffusion model. Among many types of models, the most popular ones are the linear threshold (LT) model and the independent cascade (IC) model, which are proposed in [32] with many practical application backgrounds.

In the IC model, the information diffusion consists of discrete steps. Each node has two states, active and inactive. The active means that the information has been accepted by the node. Initially, a certain set of nodes (called *seeds*) is set to be active and others are inactive. Associated with each arc (i.e., directed edge)  $(u, v)$ , there is a propagation probability  $p_{uv}$ . If  $u$  becomes active at step  $t$ , then  $u$  attempts to activate each inactive neighbor  $v$  at step  $t + 1$  with a success probability  $p_{uv}$ . Two important rules are as follows: (a) The attempting of  $u$  is allowed only at Step  $t + 1$ , not later. (b) If there are two or more nodes  $u_1, \dots, u_k$  attempting to activate  $v$ , then those attempting are considered as independent events, that is, the success probability of activating  $v$  is  $1 - (1 - p_{u_1v}) \cdot \dots \cdot (1 - p_{u_kv})$ . The diffusion process ends at the step that no inactive node is activated.

In the LT model, each node has two possible states, active and inactive. Each arc  $(u, v)$  is associated with a weight  $w_{uv}$  such that for each node  $v$ ,  $\sum_{u \in N^-(v)} w_{uv} \leq 1$

where  $N^-(v) = \{u \mid (u, v) \in E\}$ . Initially, every node  $v$  selects a threshold value  $\theta_v$  uniform-randomly from  $[0,1]$ . Meanwhile, a certain set of nodes (called *seeds*) is set to be active and others are inactive. At each subsequent step, each inactive node  $v$  evaluates the total weight of active nodes in  $N^-(v)$ . If  $\sum_{\text{active } u \in N^-(v)} w_{uv} \geq \theta_v$ , then  $v$  is activated. Otherwise,  $v$  is kept being inactive. The diffusion process ends at the step that no inactive node is activated.

When the information diffusion process ends, the expected number of active nodes is called the *influence spread*.

A problem in different information diffusion models may have different computational complexity. For example, consider the influence maximization problem, that is, given a social network with a diffusion model and an integer  $k > 0$ , find  $k$  seeds to maximize the influence spread. In a special network (called in-arborescence) with the LT model, the influence maximization is polynomial-time solvable [80]. However, the same problem in the same network with the IC model is NP-hard [47]. More surprisingly, the following is still open.

**Possible Research 1** Is there a polynomial-time good approximation (e.g., constant-approximation) for the influence maximization in general social networks with the positive influence model?

The definition of the positive influence model can be found in [74, 95], which is a special case of the general threshold model [86]. For some cases of the general threshold model, it is already proved not to have a polynomial-time constant-approximation if  $P \neq NP$  [45, 46]. However, the positive influence model is not among them.

From the above background, we may know clearly that in the traditional study of social network problems, it is important to make clear what information diffusion model lies in the background. Here, let us mention a sequence of works about rumors lying in variations of the LT or IC model [16, 24, 55, 71, 72, 91, 92, 98].

An interesting advantage of machine learning approaches is that sometimes, the information diffusion model may not be necessarily known explicitly [70].

## 2.2 Rumor

There is no universal definition of rumor, and different publications have proposed different descriptions. DiFonzo et al. [13] defines rumor as “*unverified and instrumentally relevant information statements in circulation that arise in contexts of ambiguity, danger or potential threat, and that function to help people make sense and manage risk*”. Merriam-Webster Dictionary explains rumor as “*talk or opinion widely disseminated with no discernible source, and a statement or report current without known authority for its truth*”. Xiao et al. [87] propose a definition as “*Rumor refers to the information that has not been publicly confirmed by the government or has been denied by the government. It has false, anonymous,*

*unofficial and other characteristics.*” Most definitions describe the rumor from three aspects:

1. A rumor is unverified.
2. Rumor has the power to spread
3. Rumors can cause negative effects.

This chapter focuses on debunking rumors and minimizing the spread of rumors. So we highlight the first two aspects. Therefore, we propose our rumor definition as “*rumors are disseminated information whose veracity has not been confirmed or finally verified as false.*”

A concept similar to the rumor is the fake news. Some scholars have a stricter definition of the fake news, which should be in the form of a news article [5]. Because the fake news on OSN and the rumor on OSN have fundamental similarities, that is, the fake news is also unverified when circulating and can spread widely on OSN, we do not distinguish between the rumor and the fake news in this chapter.

### **3 Machine Learning Technique Models**

#### **3.1 Conventional Machine Learning Models**

##### **SVM**

Support vector machine (SVM) was one of the most effective supervised machine learning algorithms for classification and regression tasks [53] before the rise of deep learning. SVM works by mapping data to the N-dimensional feature space and finding a hyper-plane as the decision boundary. The objective of SVM is to find a hyperplane that has the largest distance from itself to the nearest data points, a.k.a., support vectors. SVM can also work for nonlinear classification tasks by integrating kernel functions [9] (Fig. 2).

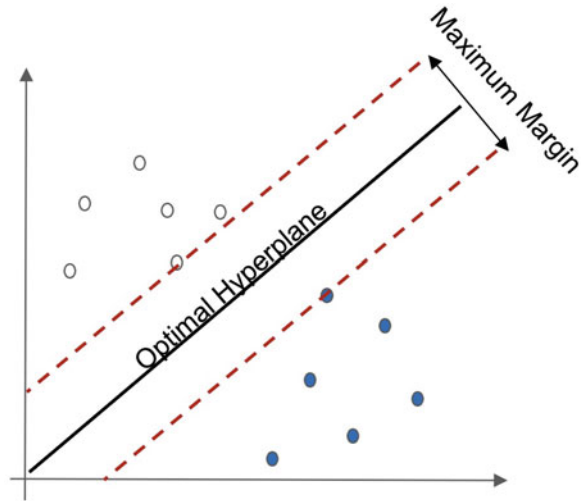
##### **Decision Tree**

The decision tree [61] uses a tree structure to represent the progress of classification or regression. When used for regression tasks, a decision tree is called a regression tree. A decision tree is composed of three types of nodes:

- Root node: representation of all input samples.
- Internal node: representation of a test on an attribute.
- Leaf node: representation of the result of the decision.

In a decision tree, a judgment is made at the inner node of the tree with a specific attribute value. The judgment result determines which branch to enter. The

Fig. 2 SVM example



algorithm ends when reaching a leaf node that represents the class labels (for the regression task, the leaf node outputs a value). Various algorithms are designed for generating a decision tree, and the most widely used are ID3, C4.5, and CART.

Figure 3 shows a decision tree on how to make a decision to buy a computer. From root node to leaf node, we evaluate the CPU model, RAM size, and storage size until we reach the leaf node as the final decision.

The decision tree model is easy to interpret and visualize. It can be applied to large datasets because of its high efficiency. But with the tree depth growing, the decision tree is prone to be overfitting. One way to overcome overfitting is pruning, which is a technique to reduce the decision complexity by removing certain parts of a tree. Another way is using a random forest to replace a single decision tree.

## Random Forest

Random forest is an ensemble learning algorithm for classification and regression. A random forest consists of decision subtrees that are trained on different samples. Each decision tree will generate its own prediction. For classification tasks, the class label selects from outputs of decision trees by majority vote. For regression tasks, it averages the output of each tree's output as a result. Compared to a single decision, a random forest is less sensitive to data variations. Therefore, a random forest is a more robust model than a decision tree and can alleviate the overfitting problem.

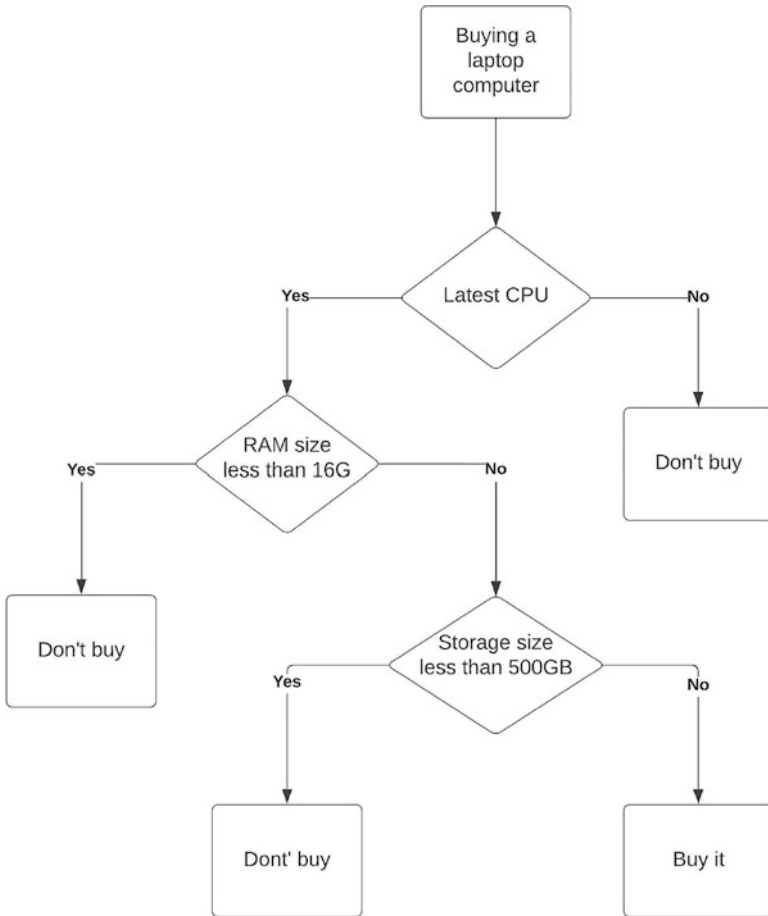


Fig. 3 Decision tree example

### Logistic Regression

Logistic regression is a supervised classification algorithm. This algorithm is often used for binary classification. The algorithm wraps the linear combination of independent attributes with the sigmoid function to force its output value between 0 and 1. For binary classification, the output can only be 0 or 1, which is decided by 0.5 as the threshold. The training stage of the algorithm aims to learn the weights of the linear combination of attributes. Besides binary logistic regression, other variants include multinomial logistic regression for multiclass classification, and ordinal regression for classification with ordered class.

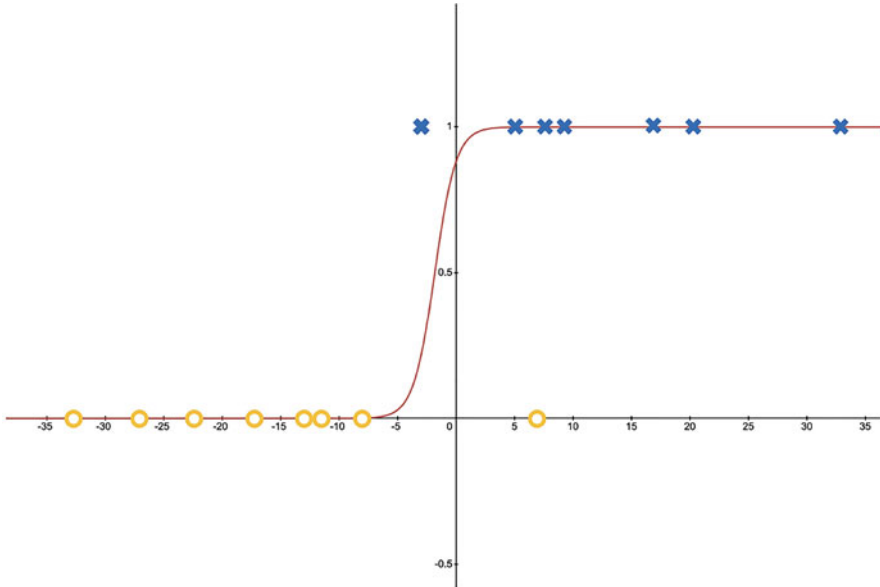


Fig. 4 Logistic regression example

Figure 4 is an example of a linear regression. Two types of samples are distinguished by fitting a sigmoid function, with 0.5 as the threshold, and those above 0.5 are classified as 1, and those below 0.5 are classified as 0.

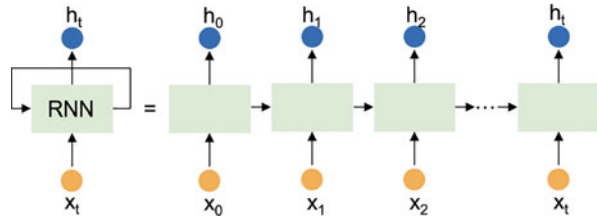
### 3.2 Neural Network Models

#### Recurrent Neural Network

A recurrent neural network (RNN) is a neural network trained on sequence data, and it is widely used in natural language processing (NLP), time-series data analysis, etc. RNN is distinguished by its structure, which recurrently links neurons. Unlike conventional neural networks, which assume inputs are independent, RNN recurrently connects neurons and can unfold with time to form a chain-like structure. The RNN neuron takes the last time step as the input of the current time step, and all neurons share parameters. That is to say, RNN has memory. However, the memory is short term since RNN suffers *vanishing* or *exploding* gradient problems when the input sequence is long.

$x$  represents the time series elements and  $h$  represents the hidden state. The time-series elements are sequentially input to the same RNN unit, and the RNN unit will generate the current hidden state based on the current input and the previous hidden state for each input. After the last time-series element is input, the generated

Fig. 5 RNN example



hidden state contains memory of the whole sequence. The two sides of the equal sign are two common representations of RNN neural network workflow, and they are equivalent

Long short-term memory (LSTM) [29] is an enhanced version of RNN that has the ability to learn long sequence data. LSTM adds several small neural networks to RNN neurons that are referred to as gates. The gates regulate the flow of information to make sure helpful information is kept and nonimportant information is discarded. In essence, the gates can be seen as an attention mechanism. Gated Recurrent Unit (GRU) [3] is a variant of LSTM. It has a simpler neuron structure but without comprising performance. Therefore, GRU has become more and more popular in recent years (Fig. 5).

## Convolution Neural Network

Convolution neural network (CNN) [39] achieves remarkable success in the computer vision domain and has been used for image classification [39], object detection [22], and face detection [63]. 1-D CNN, also called time-delay neural network, is suited for time-series data. A typical CNN architecture is a stack of convolution layers and pooling layers.

- *Convolution Layer:* The main component in CNN. It extracts features (or feature map) using learnable parameter filters (or kernels). The filters are applied along width and height to the input (for 1-D CNN only along with height), and the dot product between the overlapped part of input and filter is estimated and stored in order. In this way, the convolution layer learns the spatial features and position of the input. The result is sent to the activation function and then the pooling layer.
- *Pooling Layer:* Although convolution is effective in extracting feature maps, it also learns the position of features. If the input feature maps position changes, the model performance may drop significantly. The pooling layer aims to downsample the feature maps to make the model less sensitive to position and more robust. It receives the output from the convolution layer and applies pooling operations. Common pooling operations include average and max pooling.

By stacking convolution and pooling layers, CNN learners the local relevance of information and maps low-level features to high-level features. That is why CNN is suitable for learning image and text data (Fig. 6).



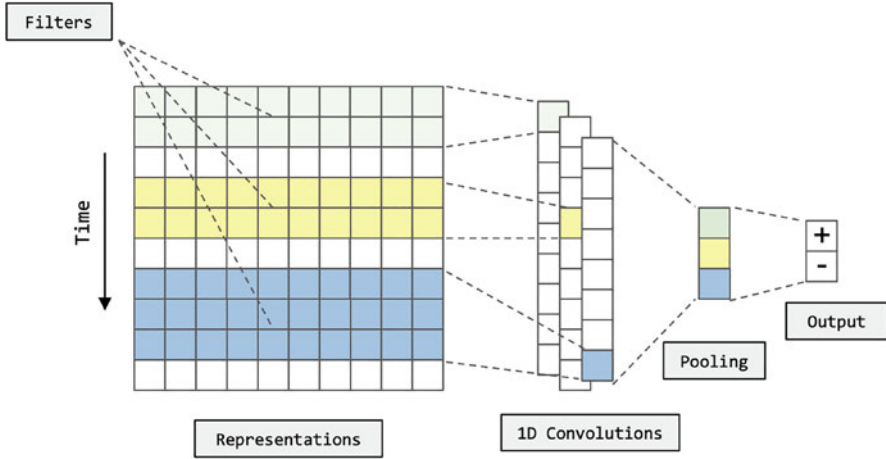


Fig. 6 1-D CNN example

## Attention

LSTM embeds the information into a fixed-length vector, regardless of how long the input is. The vector length determines the amount of information that can be stored. Although LSTM alleviates the long-term memory issue of RNN, its performance still degrades when processing long sequences. The attention mechanism is proposed by Vaswani et al. [77]. It aims to solve the information loss caused by embedding the long sequence into a fixed-length vector. The attention mechanism assigns different weights to items of the input sequence and highlights the critical parts.

## Graph Neural Network

A graph neural network, as the name implies, is a neural network that can process graph data. GNN has been used in computer vision [2], drug discovery [21], recommendation system [93], etc.

Data can be divided into Euclidean data and non-Euclidean data. Data such as text and images can be clearly represented as a grid. Text is a 1-D grid, and image pixels form the 2-D grid. The points in the grid are ordered and the number and order of neighbors are defined in advance. Traditional neural networks have achieved excellent results for tasks based on Euclidean data. While the social network is a graph, which is typical non-Euclidean data, with no grid-like structure, the nodes on the graph are not ordered, and the number of neighbors of each node is not fixed. Conventional neural networks cannot handle graph data well [7]. Therefore, GNN has received increasing attention in recent years.

When processing graph data, there are two main advantages of GNN compared to conventional neural networks. Firstly, conventional neural networks cannot handle graph data input properly because they process inputs in a predefined order, while graph nodes are not ordered. This problem is solved because GNN is insensitive to the input order of the node. Secondly, the conventional neural network cannot capture the dependency of nodes or can only treat the dependency as a node feature. While GNN updates node representation based on node connectivity, preserving the graph structure information.

The computational process of a typical graph neural network consists of two steps [89] The operations in each neural network layer can be abstracted into two steps: (i) *AGGREGATION*: aggregate neighbor nodes representations; (ii) *COMBINATION*: combine the neighbor aggregation and node itself.

Take a widely used GNN model, GCN [33] as an example. In each GCN layer, all nodes' embeddings are updated iteratively, for node  $v_i$ , its embedding is updated by the below formula:

$$\mathbf{x}'_i = \Theta^\top \sum_{j \in \mathcal{N}(v) \cup \{i\}} \frac{e_{j,i}}{\sqrt{\hat{d}_j \hat{d}_i}} \mathbf{x}_j \quad (1)$$

Here  $x$  is the current node embedding.  $\Theta$  is learnable weight matrix.  $\mathcal{N}(v)$  means all neighbor nodes of  $v_i$ . The update formula considers both  $\mathcal{N}(v)$  and  $v_i$ , thus it covers both *AGGREGATION* and *COMBINATION*. Moreover,  $e_{j,i}$  is the weight of the edge from source node  $v_j$  to  $v_i$ ,  $\hat{d}_i$  is the in-degree value of  $v_i$  plus one. The graph structure information is integrated into the node embedding  $x_i$  by considering the edge weight and node degree.

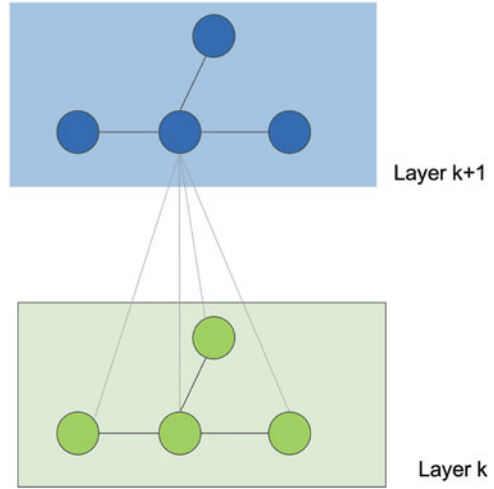
Other commonly used GNN models include GraphSage [27], GIN [89], GAT [78], etc. They use different Aggregation and Combination methods than GCN. For example, GAT uses an attention mechanism instead of a static aggregation step to aggregate the information of neighbors.

Moreover, GNN is usually stacked in multiple layers. In a  $k$ -layer GNN, every node receives  $k$ -order neighborhood information since the aggregation step is applied  $k$  times. This process can be seen, to some extent, as simulating the spread of social influence (Fig. 7).

### 3.3 Discussion

In applications of machine learning, it is very important to determine the technique model that properly fits the input–output relationship in a considered problem. For example, Tong [70] successfully established a technique model for the relationship between the attackers and protectors, so that based on historical data of input–output pairs, a strategy can be learned to compute locations of protectors against future attackers. Tong's work suggests the following possible research.

**Fig. 7** GNN updates node embedding



**Possible Research 2** In [98], a robust method is introduced to determine protector locations without knowing locations of the attackers. Based on this robust method, is it possible to establish a machine learning technique model that fits the relationship between networks and locations of protectors?

**Possible Research 3** In the literature, there are many influence types, such as adaptive influence [26, 75], group influence [97, 100], composed influence [99], community-based influence [25], and interaction-aware influence [19]. They can be extended to many types of rumors and corresponding types of protectors. Could Tong's model fit those types of rumors and protectors? If not, what new models should be constructed?

## 4 Features

### 4.1 Textural Feature

The text content is the most straightforward material for rumor detection.

Rumors are fabricated with the aim of spreading rapidly and widely. Therefore, they have some special properties compared with ordinary content. For example, rumors tend to use extreme words to attract people's attention. Based on granularity, textural features have three levels.

### **Lexical Level**

Lexical level is the word-level feature such as bi-grams, tri-grams, and bag-of-word (BoW). The words can reflect emotional tendencies also deserve attention. It is proven that rumors tend to have more negation, inferring, and tentative words [79]. Castillo et al. [10] count the question mark, exclamation mark, emoticon, etc., as features. Kwon et al. [36] utilize LIWC, a tool that counts the words in psychologically meaningful categories analyzed text, and showed rumors and nonrumors are different in terms of positive affect words, inferring action words, and cognitive words.

### **Syntactical Level**

Syntactical-level feature is sentence level feature. Include the pattern of the POS of sentence words [28, 101]. The sentence length and grammar complexity [6, 79], the sentence sentiment score [6], etc.

### **Semantic Level**

With the rise of deep learning, semantic embeddings, such as word embedding [52], are widely used, and effectiveness has been proven. Word embedding models allow us to represent words using predefined dense vectors. Each element in the vector is a parameter and will be learned using a deep neural network. Similar words will have similar vector values. Compared to the bag-of-word (BoW) model, which also represents words as vectors. BoW only concerns word counts, while word embedding takes into account the context, which means word embedding can learn the semantic information. Doc2vec [38], an extension of word embedding, is also worth mentioning. Doc2vec works well for generating embedding for short documents, such as tweets.

## ***4.2 Temporal Feature***

Temporal feature is about the pattern of the life cycle of rumors. Know et al. [35] compare the time series of rumors and nonrumors and notice that nonrumors tend to have multiple and periodic spikes in tweet volume compared to rumors, which tend to have a single prominent spike. Ma et al. [49] trace the change in frequency of specific keywords over time and notice rumor and nonrumor show different patterns.

### 4.3 Structural Feature

We can represent the rumor propagation process using a tree-like structure named propagation tree [85]. The tree is constructed based on who-replies-to-whom relationships. The root is the original message, and the other nodes are reposts. If there is a directed edge from  $m_i$  to  $m_j$ , it means  $m_j$  responds  $m_i$ .

The structure of the propagation tree, such as size, depth, node degree, etc., could be used for debunking rumors. Kwon et al. [36] compared the rumor and nonrumor propagation trees and showed rumor propagation tree tends to be a singleton. They also designed 15 structure features. Wu et al. [85] proposed a novel propagation tree that integrated user information. Wang et al. [81] evaluated rumor and nonrumor propagation tree structure from a temporal view. It shows the structures evolving processes are more distinguishing than static structures.

### 4.4 User Feature

Rumor spreader usually has low social influence, and how to use rumor attract more public attention. Celebrities are unlikely to spread rumors since it would damage their reputation. User features include single user's features, including "age," "gender," "register time," "number of follower," etc.

Kwon et al. [35] researched the relation between the social influence of rumor spreaders. They use the number of followers, friends, and tweets as a proxy of social influence, and nonrumor users show a higher feature value than rumor spreaders.

Moreover, user features benefit early rumor detection. At the early stage of rumor spread, available information is limited. The user feature is more available than other features.

## Discussion

According to the research of Kwon et al. [35], user feature and textural feature are more available at the early stage of rumor spread, and they benefit early rumor detection. While, for long-term stage, structural and temporal show better effectiveness. A single type of feature can only provide limited information and is not reliable. For example, the textural feature is the most widely used feature and has been intensively studied. However, some rumor spreader deliberately imitate the style of nonrumors. Therefore, it leaves room for the following research.

**Possible Research 4** Use not only one feature, but combine multiple features for comprehensive judgment.

## 5 Applications of Machine Learning in Rumor Controlling

With the development of Web 2.0, the role of social media users shifted from an information receiver to an information producer. Due to the role shift, rumors surged dramatically in social media platforms in recent years, which makes the rumor-controlling research become significantly important. Rumor detection and rumor blocking are two major research problems in rumor control. Rumor detection aims to distinguish rumor from genuine news also known as content-based rumor identification problem [14] while rumor blocking aims to minimize the number of users or nodes that accept (or are influenced by) the rumor in social networks. There are primarily two strategies followed for rumor blocking: first, misinformation prevention that aims to minimize the spread of rumors by launching the opposite positive cascade and second, rumor source identification that aims at detecting the possible origin(s) or source(s) of rumor propagation in social networks [20] and then clean up the rumor from the root.

### 5.1 Rumor Detection

#### Problem Statement

Given a story, which consists of a collection of messages  $m_1, m_2, \dots, m_n$ , of which  $m_1$  is the source message, and  $m_2$  to  $m_n$  are reply messages. Each message has its own properties, including textual content, image, video, URL, etc. Each message is posted by a user, who has properties such as gender, account creation time, count of followers, etc. The rumor detection problem aims to decide whether the story is a rumor or nonrumor. Therefore, the rumor detection problem is a classification task.

#### Dataset

Most of the datasets are from Twitter and Weibo.

- Twitter is a US social networking and microblogging platform that was founded in 2006. Users can send short messages of up to 280 characters on Twitter, these messages are also known as tweets. Twitter has more than 200 million daily users.
- Weibo is one of the largest social media in China, which is launched in 2009. “Weibo” means microblog in Chinese. It is a microblogging website similar to Twitter, Instagram, and Tumblr. Weibo has over 200 million daily users and over 500 million monthly users.

Details of the datasets are shown in Table 1.

**Table 1** Rumor detection dataset

Dataset	Total claim	Platform	Label	Data source
Twitter15	1490	Twitter	True rumor, false rumor, nonrumor, unverified rumors	[43]
Twitter16	818	Twitter	True rumor, false rumor, nonrumor, unverified rumors	[50]
Ma-Twitter	992	Twitter	Rumor, nonrumor	[49]
Ma-Weibo	4664	Weibo	Rumor, nonrumor	[49]
PHEME	6425	Twitter	True rumor, false rumor, nonrumor, unverified rumors	[34]
SemEval19	325	Twitter, Reddit	True, false, unverified	SemEval 2019 Task 7 data set

## Evaluation Metrics

Since the rumor detection problem is a classification one, accuracy, precision, recall, and F1 score, which are often used evaluation metrics for most classification tasks, can be applied to rumor detection problems.

Accuracy is the proportion of correct predictions. It is the most straightforward and easy-to-interpret metric. However, it does not take into account the distribution of labels. If the dataset is heavily skewed, the model always predicts the majority label with very high accuracy, but the result does not mean the model can really tell whether the input is a rumor or not.

Precision is the proportion of correctly detected rumors to all the rumor predictions. We want a model that has high precision. However, if the precision is too high, it means the model is picky and too cautious when making a prediction.

The recall represents the proportion of samples predicted as rumors to all rumor samples. However, if a model always treats the input sample as a rumor, it achieves a very high recall. The score is misleading and cannot reflect the model's performance.

Precision and recall hold a reversed relationship. In general, recall values tend to be low when precision is high and vice versa. Usually, precision and recall should not be used in isolation.

As a tradeoff for precision and recall, F1 is proposed. F1 is the harmonic mean of precision and recall. The goal of F1 is to improve precision and recall as much

as possible, and we also hope that the difference between the two is as small as possible.

Compared to precision and recall, F1 gives a more fair and comprehensive assessment. Compared to accuracy, F1 is a more robust evaluation metric since it takes into account the distribution of data and can still accurately reflect the performance of the model if the label distribution is unbalanced.

The formulas of accuracy, precision, recall, and F1 are shown below:

$$Accuracy = \frac{\text{true positive} + \text{True Negative}}{\text{All Samples}} \quad (2)$$

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \quad (3)$$

$$Recall = \frac{\text{true positive}}{\text{True Positive} + \text{False Negative}} \quad (4)$$

$$F1 = 2 \times \frac{\text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (5)$$

### Conventional Machine Learning Approach

In the early research stages, traditional machine learning methods with feature engineering approaches are popular. Castillo et al. [10] predict the credibility level by leveraging the decision tree on Twitter based on text and re-tweeting behavior and links to external resource features. Kown, Cha, and Jung [35] study the temporal, linguistic, and structural features and evaluate the performance of SVM, decision tree, and random forest, and decision tree on selected features. Wu et al. [85] proposed a graph-kernel-based SVM classifier for rumor detection. The model was trained on the features including topic, sentiment, propagation patterns, and user profiles.

### RNN-Based Approach

This is the first study to introduce RNN-based model for rumor detection on microblogs. The authors realized that the temporal and textural features of sequential text streams in social media can reflect the characteristic of rumors. First, they model the social context information of an event as a variable-length time series and applied RNN models to learn both temporal and textural features of the time series. Considering that an event could contain a large number of posts, they batch posts into time intervals and treat them as a single unit in time series. The representation of each unit is generated based on top-K TF-IDF values of vocabulary terms. Then they developed three different RNN structures to learn the time series data, which



are tanh-RNN, single-layer LSTM/GRU, and multilayer GRU. They test their model on Twitter and Weibo data to compare the performance of different RNN models. Multilayer GRU achieved the best performance (88% accuracy on Twitter dataset and 91% accuracy on Weibo dataset), demonstrating that the hidden layer can help the model to overcome noise. LSTM/GRU also overperforms the tanh-RNN, demonstrating the superiority of the gated units over the tanh unit. RvNN, which is a type of recurrent neural network for tree structure data that original application is to learn the sentence parse tree [67]. Ma et al. [51] bring RvNN to rumor detection area. Unlike other RNN models, the input of RvNN is a propagation tree rather than a temporal sequence. Therefore, RvNN can learn both the structural information of the propagation tree and the semantic content of tweets. The author proposed two variants of RvNN to learn the propagation tree using a top-down and bottom-up manner. Top-down RvNN starts from root and recursively integrates the features of parent nodes into children nodes, recursively up to leaf nodes. Finally, the pooling of all the leaf nodes is used for prediction. Bottom-up RvNN recursively integrates the features of the child nodes into the parent node starting from the leaf node until the root node. Finally, the root node is used for prediction.

### **CNN-Based Approach**

Convolutional neural networks can concentrate on local information before synthesizing it at a higher level to obtain global knowledge. CNN is commonly used in rumor detection.

CNN-based approaches usually first create a matrix using word embeddings that could represent sentences as input to the model. We could collect features between numerous consecutive words in this fashion, and weights could be shared when computing the same type of feature.

Sarkar et al. [12] developed a hierarchical architecture based on CNN to detect satire news, which attempted to capture the important information of satire in the news at the sentence and document levels. Despite the fact that they did not manually extract sentence elements to represent satire, their method produced results that were equivalent to the existing models. A single layer of CNN, on the other hand, can only create representations from a few close words. Qian et al. [58] presented a two-level convolutional neural network (TCNN) that could represent phrases in two ways and capture deep semantic information to detect whether an article was fraudulent or not. In the end, TCNN outperformed the other approach in the study. Because of its ability to extract deep information and propose a two-level representation, TCNN outperformed CNN.

### **GNN-Based Approach**

Bian et al. [4] proposed a novel GCN-based rumor source detection model Bi-GCN, which is the first attempt that applies GCN to rumor detection in social

media. Standard GCN cannot learn directed graph topology; however, direction is important for rumor detection. Bi-GCN is a novel directed GCN model to model both rumor propagation and dispersion. GCAN proposed by Lu and Li [44] uses GCN to model user propagation and use co-attention mechanism to model the correlation between the information source and other user's interaction. Wang et al. [82] proposed a content-based rumor detection model KMGCN that combines GCN and knowledge graph. KMGCN converts text content to a graph instead of a sequence to better capture nonconsecutive phrases and uses a GCN to extract the semantic representation of the graphs. Besides, KMGCN introduces real-world knowledge graphs as complementary semantic information to improve prediction performance. Dong et al. [15] proposed GCNSI, which is the first ConvGNN-based model for multiple rumor source detection problems. Compared to some other rumor source detection models, we need to know the underlying propagation model in advance, GCNSI is closer to real world since it does not rely on prior knowledge of the underlying propagation model. Song et al. [68] proposed TGNF, a GNN-based solution that works on continuous-time dynamic graphs (CTDG). TGNF captures textural, structural, and temporal features. Especially for learning temporal propagation patterns, TGNF shows superior performance than models that work on a static graph. Moreover, TGNF also integrates adversarial learning [23] framework to force the model to learn the difference between interactions rather than similarities.

### Hybrid Approach

Ajao et al. [1] developed a hybrid model of recurrent neural networks and convolutional neural networks to detect and categorize fake news messages from Twitter tweets, which recognizes acceptable features linked to fake news without prior knowledge of the subject. With the aid of a hybrid model of RNN and CNN, it automatically finds features among Twitter messages without any prior information about the topic domain or subject of conversation. It then uses text and images to identify and classify bogus news on Twitter. Because deep learning methods allow for automatic feature extraction, the associations between words in phony texts will be known without explicitly manipulating them within the network. Their approach has an accuracy rate of 82%.

Lao et al. [37] present a system that combines RNN, CNN, and GNN to capture multiple levels of rumor feature. In greater detail, the linguistic feature is captured by CNN, the temporal diffusion pattern is captured by RNN, and the nonlinear diffusion pattern is captured by GNN.

### Discussion

Each of the three types of neural networks, RNN, CNN, and GNN, has a unique set of features. RNNs are better compared to capturing patterns with linear structure,

such as the time sequence of a rumor. However, RNNs have a strict order-sensitive structure, which means that adjacent elements in the default sequence cannot be interchanged. CNN can also capture linear structure features, but the presence of a filter enables CNN to find local patterns more effectively, and unlike RNNs, they are strictly order-sensitive. Moreover, CNN usually runs much faster than RNN on GPU. GNN, as a type of neural network that has gained popularity in recent years, has garnered considerable interest. It is capable of recognizing the graph's global structure, which is not possible with RNN or CNN. Nonetheless, it is not a perfect substitute for RNN and CNN. RNN/CNN-based learning of linear rumor propagation structures remains a viable complement and enhancement to the GNN-based approach.

## Future Direction

### Model Interpretability

Usually, the more complex a model is the more difficult it is to interpret. Decision trees, for example, are highly interpretable by making only basic conditional judgments. Neural networks, with a large number of parameters and multilayer structure, have a strong fitting ability, which also makes the model very complex and turns it into a black box.

Most of the current deep learning-based rumor detection model research merely pursues performance and ignores the problem of model interpretability. Some questions still need to be answered.

**Possible Research 5** How does the model make predictions? What features play the most important role when making the decision? What is the glass ceiling of the deep learning model?

Studying the interpretability of the model helps us to understand the mechanism of rumor propagation, which can guide us in designing and collecting features and improving the model.

### Early Detection and Knowledge Base

Due to the harm of rumor spreading, it is the consensus of everyone to stop the spread of rumors as soon as possible. However, early rumor detection is challenging since the available information is limited during the early stages of rumor spreading. Introducing knowledge from an external source, such as a knowledge base (KB), is a feasible solution. KBs store entity information in a triple format. Each triple represents two entities and their relationship. KB not only stores a wide range of entity information but also emphasizes the connections between them.

**Possible Research 6** Due to the wide variety of OSN content, the content could be structured, unstructured, text, image, video, URL, etc. It is impossible to have a

KB cover all the OSN contents. For the uncovered part, rumor debunking is still a challenge.

## Dynamic Graph

Social network is a typical dynamic graph. A dynamic graph denotes a graph that the nodes and edges and features can change over time. For example, in social networks, new users may join, old users may leave, and users may establish new relations or remove old relations. Dynamic graph introduced can lead to new graph topology and new node profiles. A dynamic graph-friendly model should be able to capture temporal changes of graph and incrementally update results. Moreover, there are two categories of dynamic graphs: discrete-time dynamic graphs (DTDG), which are composed of a sequence of snapshots taken at interval time; and continuous-time dynamic graphs (CTDG), which are composed of a list of timed node or edge events. It is obvious that CTDG is more general. Some representative CTDG-based GNN models were also proposed. For instance, TGAT [88] and TGN [60]. Based on TGAT, Song et al. [68] proposed a CTDG-based fake news detection solution.

**Possible Research 7** The current rumor detection solutions are still mainly based on static graphs, and exploring dynamic graph models is a valuable direction.

## 5.2 Rumor Source Identification

### Problem Statement

Rumor source identification focuses on locating the propagation source(s) or seed node(s) of rumor in social network. This problem aims to learn the reverse dynamics of the diffusion process means tracing the diffusion dynamics back to its initial state and identifying the first nodes that started spreading the rumor [64]. The ability to quickly identify the source(s) of rumor can help in controlling the spread of rumor at an early stage by cutting off the critical paths of rumor diffusion. This research is also used in a wide variety of domains such as detecting the source of epidemics to control infection spreading, finding the source of a computer virus in a network, and locating gas leakage source in wireless sensor network [31]. Generally, the methods of rumor source identification found in the literature take the information propagation/diffusion model, network structure, and the states of a portion of nodes into consideration while emerging studies try to identify source(s) without knowing the underlying propagation model.

Commonly used models for rumor propagation in social networks are IC model and epidemic models. Widely adopted epidemic models for rumor propagation are (susceptible-infected (SI) model, susceptible-infected-susceptible (SIS) model, susceptible-infected-recovered (SIR) model, and susceptible-exposed-infected-

recovered (SEIR). According to the model, the nodes in the graph are in one of the following states: (S) who are susceptible to rumor but not yet activated; infected (I) who has been activated or infected by the rumor and are infectious, that is, they will spread the rumor and recovered (R) who are removed from consideration after being in the full activation period, as they will not pass the rumor to their neighbors anymore. Given an initial set of source nodes, the above propagation models are utilized for generating the state of the network and based on the type of network observation rumor sources are determined.

Network observation provides knowledge about the different states of nodes in the network while the diffusion process is undergoing or completed. Complete observation of the network provides the exact state for each node in the network at a given moment. Snapshot-based observation provides the details of activated nodes at the time of the snapshot, but cannot discriminate between susceptible or recovered node. To overcome this problem, multiple snapshots are taken at varying time slots to get sufficient knowledge of the network. In monitor-based observation, initially monitor or sensor nodes are inserted into the network, which works as an observer for evolutionary propagation in the network. Monitor nodes collect the information that passes through them and also their infection time is gathered. In this type of observation, the accuracy to detect rumor sources depends on the number of monitors placed in the network [66].

In the literature, we can find a vast amount of algorithm-based methods for source identification problem [54, 90, 96]. For the scope of this chapter, we will focus on machine learning-based approaches to this problem.

## Conventional Machine Learning Approach

We aim to identify the source of the rumor based on the state of nodes as well as the underlying network structure using the prior information about the probabilistic rumor propagation model. Since there is no additional information (i.e., a uniform prior), the maximum likelihood (ML) estimator is utilized that minimizes the estimation error, that is, maximizes the correct source detection probability. Research focused on this approach first identifies a computationally tractable representation of the ML estimator if possible and evaluates the source detection probability of such an estimator [65]. The majority of the work based on this approach focuses on finding the single source in the network.

## GNN-Based Approach

Shah et al. [64] proposed a GNN-based approach for finding the source of epidemic, namely, patient zero in general graph when the disease propagates in the networks based on SIR and SEIR model. One-hot encoded node states, that is,  $x_i \in \{0, 1\}^M$ , where  $M$  is the number of possible states for a node where state of a node is either  $\{S, I, R\}$  or  $\{S, E, I, R\}$  are the input to the GNN. The output is the probability

of a node being a patient zero. They showed with experimental analysis that GNN performs better compared to the famous algorithm-based approach called dynamic message passing as GNNs are model-agnostic and do not require access to the epidemic dynamics parameters or the time  $t$  of the graph snapshot. Also, inference through GNN is 100 time faster compared to algorithm-based methods. Li et al. [42] also proposed a GNN-based model called Source Identification Graph Convolutional Network (SIGN) when rumor diffusion follows the SI model for single-source identification problem under the complete snapshot. Their model is based on the idea that the source should be in the center of the infection subgraph and far from the uninfected frontier also known as rumor centrality.

Wang et al. [83] proposed for the first time a semi-supervised learning model called Label Propagation-based Source Identification (LPSI) for multiple source detection method when the underlying rumor propagation model is unknown. It encodes the state of the node at the time  $t$  of snapshot, +1 if node is infected otherwise  $-1$ . Based on the propagation probability of each node and state of nodes at time  $t$ , state of nodes at time  $t + 1$  is determined. The output is a label for each node indicating the probability of a node being an infection source. LPSI encodes only an integer for each node that is insufficient to express the structural information of the network and also the time of the snapshot has to be known. To improve upon these deficiencies, Dong et al. [14] proposed a GNN-based model, namely, Graph Convolutional Networks-based Source Identification (GCNSI) to locate multiple rumor sources without prior knowledge of the underlying propagation model. They assign a multidimensional vector for each node for input to the GCN. One feature is the infection state of the node, and other feature captures the rumor centrality and source prominence: nodes surrounded by a larger proportion of infected nodes are more likely to be rumor sources. They also compared the performance of GCNSI with the algorithm-based approach, where GCNSI outperformed the algorithm-based methods.

## Dataset

Both real-world networks and synthetic networks are used in the literature to study the methods proposed for source identification problem. In Table 2 dataset name and its source, the papers discussed above that are using the dataset, number of nodes and edges in that dataset, along with the graph density, that is, the ratio between the edges present in a graph and the maximum number of edges that the graph can contain, are average clustering coefficient that can be defined as  $\sum_{i=1}^{|V|} C_i$ , where  $C_i$  is the clustering coefficient of each node  $i$  in the graph defined as  $C_i = \frac{n_i}{k_i}$ , where  $n_i$  is the number of edges between the  $k_i$  neighbors of node  $i$ . Other than that we also show whether the particular dataset is used for multisource detection or single-sourced detection or both and type of diffusion model adopted by the papers for rumor source identification problem. The datasets in the table are arranged in ascending order of nodes.

**Table 2** Real-world datasets used for rumor source identification in social networks.

Dataset and Data Source	Dataset used by papers	Description	#Nodes	#Edges	Density	Average clustering coefficient	Number of sources	Diffusion Model
Karate [94]	[14]	The dataset contains social ties among the members of a university karate club collected by Wayne Zachary in 1977	34	78	0.139037	0.570638	multiple	model independent
Dolphin [48]	[14]	A social network of bottlenose dolphins, where an edge represents frequent associations between dolphins	62	159	0.0840825		multiple	model independent
Cuebig	[64]	co-location graph and simulations of an epidemic with the natural progression of COVID-19	2689	30376	–	–	single	SIR, SEIR
ego-Facebook [41]	[14]	This dataset consists of friends lists from Facebook	4039	88234	–	0.6055	multiple	model independent
Western US Power Grid [84]	[14]	An undirected unweighted representation of the topology of the Western States Power Grid of the United States	4941	6594	0.000540303	0.0801036	multiple	model independent

## Evaluation Metrics

Top-k accuracy measures that rumor source can be retrieved among the k nodes with the highest probability of being the rumor source. If one of them is a true label, it classifies the prediction as correct. Top 1 accuracy is a special case, in which only the highest probability prediction is taken into account.

## 5.3 Misinformation Prevention

### Problem Statement

Misinformation Prevention problem source from the Information Maximization (IM) problem proposed by Kempe et al. [32]. The authors also propose two basic diffusion models, Independent Cascade (IC) model and Linear Threshold model. Based on the work of Kempe et al., IM problem aims to select the optimal seed node set under cardinality limitation and maximize the influence on social network.

Misinformation Prevention (MP) problem, also named Misinformation Containment Problem, or Least Cost Rumor Blocking Problem in some research, is proposed as a variant of the IM problem. As a variation of the IM problem, the MP problem was first proposed by Budak [8] et al. There are two competing cascades on social network, the rumor cascade and positive cascade. MP problem aims to minimize the number of nodes influenced by rumor cascade by selecting positive seed set called protector nodes under cardinality limitation. The MP problem is extensively researched under the IC and LT model. Budak et al. prove the MP problem is a submodular optimization problem when there are two cascades, which guarantees a  $1 - 1/e$  approximation greedy algorithm exists [8]. However, computing the cascade influence is #P-hard, making it hard to evaluate the objective function of MP problem [11]. A breakthrough comes from the reverse sampling technology proposed by C. Borg et al. Based on reverse sampling, a series of solutions are proposed in [69, 73, 76].

### Machine Learning-Based Approaches

Existing research assumes the underlying diffusion model is already known, for instance, IC or LT model. However, in the real world, the underlying diffusion could be complicated, leading to the existing solution's application range being limited.

To tackle the MP problem without knowing the underlying diffusion model in advance, Tong [70] et al. propose a novel method named StratLearner. The core idea is that to parameterize the objective function of the MP problem, the algorithm takes historical attackers and optimal protector pairs as input to learn how a strategy can maximize the parameterized objective function. Tong adapted SVM to train the model and achieve state-of-the-art performance.



**Possible Research 8** Currently, there are relatively few solutions based on machine learning in this area, but it is a direction worth exploring.

## 6 Conclusion

In this chapter, we made a comprehensive survey on research works aimed at issues on widespread rumors over the online social network. We first introduced basic concepts, including OSN and rumor, then explained machine learning models and features. Then, from the perspective of machine learning, we reviewed works in rumor detection, rumor source detection, and rumor prevention, which are the three important research areas for debunking rumors or limiting rumor spread. We emphasized public datasets, conventional machine learning-based solutions, and deep learning-based solutions, including the latest graph neural network-based solutions. Meanwhile, we identified several possible research directions for future study.

## References

1. Ajao, O., Bhowmik, D., Zargari, S.: Fake news identification on twitter with hybrid CNN and RNN models. In: Proceedings of the 9th International Conference on Social Media and Society, pp. 226–230 (2018)
2. Ashual, O., Wolf, L.: Specifying object attributes and relations in interactive scene generation. In Proceedings of the IEEE/CVF International Conference on Computer Vision, pp. 4561–4569 (2019)
3. Bahdanau, D., Cho, K., Bengio, Y.: Neural machine translation by jointly learning to align and translate (2014). arXiv preprint arXiv:1409.0473.
4. Bian, T., Xiao, X., Xu, T., Zhao, P., Huang, W., Rong, Y., Huang, J.: Rumor detection on social media with bi-directional graph convolutional networks. In: Proceedings of the AAAI Conference on Artificial Intelligence, vol. 34, p. 549–556 (2020)
5. Bondielli, A., Marcelloni, F.: A survey on fake news and rumour detection techniques. Inform. Sci. **497**, 38–55 (2019)
6. Briscoe, E.J., Appling, D.S., Hayes, H.: Cues to deception in social media communications. In: 2014 47th Hawaii International Conference on System Sciences, pp. 1435–1443. IEEE (2014)
7. Bronstein, M.M., Bruna, J., LeCun, Y., Szlam, A., Vandergheynst, P.: Geometric deep learning: going beyond Euclidean data. IEEE Signal Process. Mag. **34**(4), 18–42 (2017)
8. Budak, C., Agrawal, D., El Abbadi, A.: Limiting the spread of misinformation in social networks. In: Proceedings of the 20th International Conference on World Wide Web, pp. 665–674 (2011)
9. Burges, C.J.: A tutorial on support vector machines for pattern recognition. Data Mining Knowl. Discovery **2**(2), 121–167 (1998)
10. Castillo, C., Mendoza, M., Poblete, B.: Information credibility on twitter. In: Proceedings of the 20th International Conference on World Wide Web, pp. 675–684 (2011)
11. Chen, W., Wang, C., Wang, Y.: Scalable influence maximization for prevalent viral marketing in large-scale social networks. In: Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1029–1038 (2010)

12. De Sarkar, S., Yang, F., Mukherjee, A.: Attending sentences to detect satirical fake news. In: Proceedings of the 27th International Conference on Computational Linguistics, pp. 3371–3380 (2018)
13. DiFonzo, N., Bordia, P.: Rumor, gossip and urban legends. *Diogenes* **54**(1), 19–35 (2007)
14. Dong, M., Zheng, B., Quoc Viet Hung, N., Su, H., Li, G.: Multiple rumor source detection with graph convolutional networks. In: Proceedings of the 28th ACM International Conference on Information and Knowledge Management, CIKM '19, pp. 569–578. Association for Computing Machinery, New York (2019)
15. Dong, M., Zheng, B., Quoc Viet Hung, N., Su, H., Li, G. (2019). Multiple rumor source detection with graph convolutional networks. In: Proceedings of the 28th ACM International Conference on Information and Knowledge Management, pp. 569–578 (2019)
16. Fan, L., Lu, Z., Wu, W., Thuraisingham, B.M., Ma, H., Bi, Y.: Least cost rumor blocking in social networks. In: ICDCS, pp. 540–549. IEEE (2013)
17. Fan, L., Wu, W., Xing, K., Lee, W.: Precautionary rumor containment via trustworthy people in social networks. *Discret. Math. Algorithms Appl.* **8**(1), 165004:1–165004:18 (2016)
18. Fan, L., Wu, W., Zhai, X., Xing, K., Lee, W., Du, D.-Z.: Maximizing rumor containment in social networks with constrained time. *Soc. Netw. Anal. Min.* **4**(1), 214 (2014)
19. Gao, C., Gu, S., Yang, R., Wu, W., Xu, D.: Interaction-aware influence maximization and iterated sandwich method. *Theor. Comput. Sci.* **821**, 23–33 (2020)
20. Garg, P., Wu, W.: Social network analysis and applications: a review of the broad research aspects of social network structure. *Discrete Math. Algorithms Appl.* **14**(6), 2230001 (2022)
21. Gaudelet, T., Day, B., Jamasb, A.R., Soman, J., Regep, C., Liu, G., Hayter, J.B., Vickers, R., Roberts, C., Tang, J., et al.: Utilizing graph machine learning within drug discovery and development. *Briefings Bioinform.* **22**(6), bbab159 (2021)
22. Girshick, R., Donahue, J., Darrell, T., Malik, J.: Rich feature hierarchies for accurate object detection and semantic segmentation. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 580–587 (2014)
23. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y.: Generative adversarial nets. In: Advances in Neural Information Processing Systems, vol. 27 (2014)
24. Guo, J., Chen, T., Wu, W.: A multi-feature diffusion model: rumor blocking in social networks. *IEEE/ACM Trans. Netw.* **29**(1), 386–397 (2021)
25. Guo, J., Wu, W.: Influence maximization: seeding based on community structure. *ACM Trans. Knowl. Discov. Data* **14**(6), 66:1–66:22 (2020)
26. Guo, J., Wu, W.: Adaptive influence maximization: If influential node unwilling to be the seed. *ACM Trans. Knowl. Discov. Data* **15**(5), 84:1–84:23 (2021)
27. Hamilton, W., Ying, Z., Leskovec, J.: Inductive representation learning on large graphs. In: Advances in Neural Information Processing Systems, vol. 30 (2017)
28. Hassan, A., Qazvinian, V., Radev, D.: What's with the attitude? Identifying sentences with attitude in online discussions. In: Proceedings of the 2010 Conference on Empirical Methods in Natural Language Processing, pp. 1245–1255 (2010)
29. Hochreiter, S., Schmidhuber, J.: Long short-term memory. *Neural Comput.* **9**(8), 1735–1780 (1997)
30. Jiang, Y., Bosch, N., Baker, R.S., Paquette, L., Ocumpaugh, J., Andres, J.M., Alexandra, L., Moore, A.L., Biswas, G.: Expert feature-engineering vs. deep neural networks: which is better for sensor-free affect detection? In: International Conference on Artificial Intelligence in Education, pp. 198–211. Springer, Berlin (2018)
31. Jin, R., Wu, W.: Schemes of propagation models and source estimators for rumor source detection in online social networks: a short survey of a decade of research. *Discrete Math. Algorithms Appl.* **13**(4), 2130002 (2021)
32. Kempe, D., Kleinberg, J., Tardos, É.: Maximizing the spread of influence through a social network. In: Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 137–146 (2003)

33. Kipf, T.N., Welling, M.: Semi-supervised classification with graph convolutional networks (2016). arXiv preprint arXiv:1609.02907
34. Kochkina, E., Liakata, M., Zubiaga, A.: All-in-one: multi-task learning for rumour verification (2018). arXiv preprint arXiv:1806.03713
35. Kwon, S., Cha, M., Jung, K.: Rumor detection over varying time windows. *PLoS One* **12**(1), e0168344 (2017)
36. Kwon, S., Cha, M., Jung, K., Chen, W., Wang, Y.: Prominent features of rumor propagation in online social media. In: 2013 IEEE 13th International Conference on Data Mining, pp. 1103–1108. IEEE (2013)
37. Lao, A., Shi, C., Yang, Y.: Rumor detection with field of linear and non-linear propagation. In: Proceedings of the Web Conference 2021, pp. 3178–3187 (2021)
38. Le, Q., Mikolov, T.: Distributed representations of sentences and documents. In: International Conference on Machine Learning, pp. 1188–1196. PMLR (2014)
39. LeCun, Y., Bottou, L., Bengio, Y., Haffner, P.: Gradient-based learning applied to document recognition. *Proc. IEEE* **86**(11), 2278–2324 (1998)
40. Lee, B.: 5g networks and covid-19 coronavirus: here are the latest conspiracy theories (2020). Forbes. Retrieved from, 14
41. Leskovec, J., McAuley, J.: Learning to discover social circles in ego networks. In: Pereira, F., Burges, C., Bottou, L., Weinberger, K. (eds.) *Advances in Neural Information Processing Systems*, vol. 25. Curran Associates (2012)
42. Li, L., Zhou, J., Jiang, Y., Huang, B.: Propagation source identification of infectious diseases with graph convolutional networks. *J. Biomed. Inform.* **116**, 103720 (2021)
43. Liu, X., Nourbakhsh, A., Li, Q., Fang, R., Shah, S.: Real-time rumor debunking on twitter. In: Proceedings of the 24th ACM International On Conference on Information and Knowledge Management, pp. 1867–1870 (2015)
44. Lu, Y.-J., Li, C.-T.: GCAN: graph-aware co-attention networks for explainable fake news detection on social media (2020). arXiv preprint arXiv:2004.11648.
45. Lu, Z., Zhang, W., Wu, W., Fu, B., Du, D.-Z.: Approximation and inapproximation for the influence maximization problem in social networks under deterministic linear threshold model. In: *ICDCS Workshop*, pp. 160–165. IEEE (2011)
46. Lu, Z., Zhang, W., Wu, W., Kim, J., Fu, B.: The complexity of influence maximization problem in the deterministic linear threshold model. *J. Comb. Optim.* **24**(3), 374–378 (2012)
47. Lu, Z., Zhang, Z., Wu, W.: Solution of Bharathi-Kempe-Salek conjecture for influence maximization on arborescence. *J. Comb. Optim.* **33**(2), 803–808 (2017)
48. Lusseau, D., Schneider, K., Boisseau, O.J., Haase, P., Slooten, E., Dawson, S.M.: The bottlenose dolphin community of doubtful sound features a large proportion of long-lasting associations. *Behav. Ecol. Sociobiol.* **54**(4), 396–405 (2003)
49. Ma, J., Gao, W., Mitra, P., Kwon, S., Jansen, B. J., Wong, K.-F., Cha, M.: Detecting rumors from microblogs with recurrent neural networks (2016)
50. Ma, J., Gao, W., Wei, Z., Lu, Y., Wong, K.-F.: Detect rumors using time series of social context information on microblogging websites. In: Proceedings of the 24th ACM International on Conference on Information and Knowledge Management, pp. 1751–1754 (2015)
51. Ma, J., Gao, W., Wong, K.-F.: Rumor Detection on Twitter with Tree-Structured Recursive Neural Networks. Association for Computational Linguistics (2018)
52. Mikolov, T., Chen, K., Corrado, G., Dean, J.: Efficient estimation of word representations in vector space (2013). arXiv preprint arXiv:1301.3781
53. Mountrakis, G., Im, J., Ogole, C. (2011). Support vector machines in remote sensing: a review. *ISPRS J. Photogramm. Remote Sensing* **66**(3), 247–259
54. Nguyen, D.T., Nguyen, N.P., Thai, M.T.: Sources of misinformation in online social networks: who to suspect? In: MILCOM 2012—2012 IEEE Military Communications Conference, pp. 1–6 (2012)
55. Ni, Q., Guo, J., Huang, C., Wu, W.: Community-based rumor blocking maximization in social networks: algorithms and analysis. *Theor. Comput. Sci.* **840**, 257–269 (2020)

56. Pallavicini, F., Cipresso, P., Mantovani, F.: Beyond sentiment: how social network analytics can enhance opinion mining and sentiment analysis. In: *Sentiment Analysis in Social Networks*, pp. 13–29. Elsevier, Amsterdam (2017)
57. Perrin, A.: Social media usage. *Pew Res. Center* **125**, 52–68 (2015)
58. Qian, F., Gong, C., Sharma, K., Liu, Y.: Neural user response generator: fake news detection with collective user intelligence. In: *IJCAI*, vol. 18, pp. 3834–3840 (2018)
59. Ramshree, K.: A survey of data mining techniques for social network analysis. *Softw. Eng.* **9**(1), 4–6 (2017)
60. Rossi, E., Chamberlain, B., Frasca, F., Eynard, D., Monti, F., Bronstein, M.: Temporal graph networks for deep learning on dynamic graphs (2020). arXiv preprint arXiv:2006.10637
61. Safavian, S.R., Landgrebe, D.: A survey of decision tree classifier methodology. *IEEE Trans. Syst. Man Cybern.* **21**(3), 660–674 (1991)
62. Satariano, A., Alba, D.: Burning cell towers, out of baseless fear they spread the virus. *The New York Times* 11 (2020)
63. Schroff, F., Kalenichenko, D., Philbin, J.: Facenet: a unified embedding for face recognition and clustering. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 815–823 (2015)
64. Shah, C., Dehmamy, N., Perra, N., Chinazzi, M., Barab’asi, A.L., Vespignani, A., Yu, R.: Finding patient zero: Learning contagion source with graph neural networks (2020). ArXiv, abs/2006.11913
65. Shah, D., Zaman, T.: Rumors in a network: who’s the culprit? *IEEE Trans. Inform. Theory* **57**(8), 5163–5181 (2011)
66. Shelke, S., Attar, V.: Source detection of rumor in social network—a review. *Online Soc. Netw. Media* **9**, 30–42 (2019)
67. Socher, R., Huval, B., Manning, C.D., Ng, A.Y.: Semantic compositionality through recursive matrix-vector spaces. In: *Proceedings of the 2012 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning*, pp. 1201–1211 (2012)
68. Song, C., Shu, K., Wu, B.: Temporally evolving graph neural network for fake news detection. *Inform. Process. Manag.* **58**(6), 102712 (2021)
69. Tong, A., Du, D.-Z., Wu, W.: On misinformation containment in online social networks. In: *Advances in Neural Information Processing Systems*, vol. 31 (2018)
70. Tong, G.: Stratlearner: learning a strategy for misinformation prevention in social networks. In: *Advances in Neural Information Processing Systems*, vol. 33, pp. 15546–15555 (2020)
71. Tong, G., Wu, W., Du, D.-Z.: Distributed rumor blocking with multiple positive cascades. *IEEE Trans. Comput. Soc. Syst.* **5**(2), 468–480 (2018)
72. Tong, G., Wu, W., Guo, L., Li, D., Liu, C., Liu, B., Du, D.-Z.: An efficient randomized algorithm for rumor blocking in online social networks. In: *INFOCOM*, pp. 1–9. IEEE (2017)
73. Tong, G., Wu, W., Guo, L., Li, D., Liu, C., Liu, B., Du, D.-Z.: An efficient randomized algorithm for rumor blocking in online social networks. *IEEE Trans. Netw. Sci. Eng.* **7**(2), 845–854 (2017)
74. Tong, G., Wu, W., Pardalos, P.M., Du, D.-Z.: On positive-influence target-domination. *Optim. Lett.* **11**(2), 419–427 (2017)
75. Tong, G., Wu, W., Tang, S., Du, D.-Z.: Adaptive influence maximization in dynamic social networks. *IEEE/ACM Trans. Netw.* **25**(1), 112–125 (2017)
76. Tong, G.A., Du, D.-Z.: Beyond uniform reverse sampling: a hybrid sampling technique for misinformation prevention. In: *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, pp. 1711–1719. IEEE (2019)
77. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, Ł., Polosukhin, I.: Attention is all you need. In: *Advances in Neural Information Processing Systems*, vol. 30 (2017)
78. Veličković, P., Cucurull, G., Casanova, A., Romero, A., Lio, P., Bengio, Y.: Graph attention networks (2017). arXiv preprint arXiv:1710.10903

79. Vosoughi, S., Mohsenvand, M.N., Roy, D.: Rumor gauge: predicting the veracity of rumors on twitter. *ACM Trans. Knowl. Discovery Data* **11**(4), 1–36 (2017)
80. Wang, A., Wu, W., Cui, L.: On Bharathi-Kempe-Salek conjecture for influence maximization on arborescence. *J. Comb. Optim.* **31**(4), 1678–1684 (2016)
81. Wang, S., Kong, Q., Wang, Y., Wang, L.: Enhancing rumor detection in social media using dynamic propagation structures. In: 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 41–46. IEEE (2019)
82. Wang, Y., Qian, S., Hu, J., Fang, Q., Xu, C.: Fake news detection via knowledge-driven multimodal graph convolutional networks. In: Proceedings of the 2020 International Conference on Multimedia Retrieval, pp. 540–547 (2020)
83. Wang, Z., Wang, C., Pei, J., Ye, X.: Multiple source detection without knowing the underlying propagation model. In: Proceedings of the AAAI Conference on Artificial Intelligence, 31(1) (2017)
84. Watts, D.J., Strogatz, S.H.: Collective dynamics of small-world networks. *Nature* **393**(6684), 440–442 (1998)
85. Wu, K., Yang, S., Zhu, K.Q.: False rumors detection on Sina Weibo by propagation structures. In: 2015 IEEE 31st International Conference on Data Engineering, pp. 651–662. IEEE (2015)
86. Wu, W., Du, H., Wang, H., Duan, Z., Tian, C.: On general threshold and general cascade models of social influence. *J. Comb. Optim.* **35**(1), 209–215 (2018)
87. Xiao, Y., Li, W., Qiang, S., Li, Q., Xiao, H., Liu, Y.: A rumor & anti-rumor propagation model based on data enhancement and evolutionary game. *IEEE Trans. Emer. Topics Comput.* **10**(2), 690–703 (2020)
88. Xu, D., Ruan, C., Korpeoglu, E., Kumar, S., Achan, K.: Inductive representation learning on temporal graphs (2020). arXiv preprint arXiv:2002.07962.
89. Xu, K., Hu, W., Leskovec, J., Jegelka, S.: How powerful are graph neural networks? (2018). arXiv preprint arXiv:1810.00826
90. Xu, W., Chen, H.: Scalable rumor source detection under independent cascade model in online social networks. In: 2015 11th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), pp. 236–242 (2015)
91. Yan, W., Li, D., Wu, W., Du, D.-Z., Wang, Y.: Minimizing influence of rumors by blockers on social networks: algorithms and analysis. *IEEE Trans. Netw. Sci. Eng.* **7**(3), 1067–1078 (2020)
92. Yan, W., Li, Y., Wu, W., Li, D., Wang, Y.: Rumor blocking through online link deletion on social networks. *ACM Trans. Knowl. Discov. Data* **13**(2), 16:1–16:26 (2019)
93. Ying, R., He, R., Chen, K., Eksombatchai, P., Hamilton, W.L., Leskovec, J.: Graph convolutional neural networks for web-scale recommender systems. In: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, pp. 974–983 (2018)
94. Zachary, W.W.: An information flow model for conflict and fission in small groups. *J. Anthropol. Res.* **33**, 452–473 (1977)
95. Zhang, W., Wu, W., Wang, F., Xu, K.: Positive influence dominating sets in power-law graphs. *Soc. Netw. Anal. Min.* **2**(1), 31–37 (2012)
96. Zhang, Z., Xu, W., Wu, W., Du, D.-Z.: A novel approach for detecting multiple rumor sources in networks with partial observations. *J. Comb. Optim.* **33**(1), 132–146 (2017)
97. Zhu, J., Ghosh, S., Wu, W.: Group influence maximization problem in social networks. *IEEE Trans. Comput. Soc. Syst.* **6**(6), 1156–1164 (2019)
98. Zhu, J., Ghosh, S., Wu, W.: Robust rumor blocking problem with uncertain rumor sources in social networks. *World Wide Web* **24**(1), 229–247 (2021)
99. Zhu, J., Ghosh, S., Zhu, J., Wu, W.: Near-optimal convergent approach for composed influence maximization problem in social networks. *IEEE Access* **7**, 142488–142497 (2019)
100. Zhu, J., Grosh, S., Wu, W., Gao, C.: Profit maximization under group influence model in social networks. In: CSoNet, pp. 108–119. Springer, Berlin (2019)
101. Zubiaga, A., Liakata, M., Procter, R.: Learning reporting dynamics during breaking news for rumour detection in social media (2016). arXiv preprint arXiv:1610.07363

# Strategic Communication as a Mean for Countering Hybrid Threats



Konstantinos Balomenos

## 1 Introduction

Recently, the international security environment has changed dramatically and as a result, the global community is facing with new security challenges and threats. As Robert Kagan points out in his book, “The Jungle Grows Back: America and Our Imperiled

World” [6], the world as we know, is changing fast and new actors are emerging in global politics. Today the jungle is growing back, history is returning, and we are witnessing a time when nations are reverting to the old and traditional geopolitical patterns. Great-power spheres of interests and geopolitical ambitions are creating international instability and regional conflicts [6].

One of the most important threats to international peace and security is hybrid warfare.

Hybrid warfare is a type of war in which all available resources of a state or a nonstate actor are used in combination with conventional, unconventional (unorthodox), and political means. These actors can act in both the physical, digital, and cognitive domains, and can use a variety of strategies and tactics to achieve their strategic objectives and finally, to undermine and destabilize their opponent [7].

In particular, the hybrid actors (states, teams, individuals) use means and unconventional techniques, such as covert military operations and soft power tactics, in order to exploit the vulnerabilities of the opponent without violating the limits of deterrence, which would lead to total war and finally to achieve his coercion.

---

K. Balomenos (✉)

National Defence Policy & International Relations—Hellenic Ministry of National Defence, Peristeri of Athens, Greece

e-mail: [konmpalo@otenet.gr](mailto:konmpalo@otenet.gr); [gd@mod.mil.gr](mailto:gd@mod.mil.gr)

These tactics referred to a conflict mode that is called as “gray zone conflict.” Actors in the gray zone are, employing sequences of gradual steps to secure strategic leverage. The efforts remain below thresholds that would generate a powerful response, but nonetheless are forceful and deliberate, calculated to gain measurable traction over time [8]. Others argue that, the gray zone is characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war [9]. In the same frame, gray zone conflicts, involve some aggression or use of force, but in many aspects their defining characteristic is ambiguity about the ultimate objectives, the participants, whether international treaties and norms have been violated, and the role that military forces should play in response [10].

The toolkit for coercion below the level of direct warfare includes informational and psychological operations, political coercion, economic coercion, cyber operations, proxy support, and provocation by state-controlled forces [11].

From the above, it is understandable that most hybrid warfare strategies are related to information and communication. Communication is a component of all operations and its effective use is crucial during informational and psychological operations. Information dominates in all fields of operations; therefore, it is paramount for a manager of hybrid threats and crises to understand the information environment in which hybrid operations are conducted and how the hybrid actors use communication to influence different forms of decision-making and undermine citizens’ trust in their leadership.

In this vein, the author will use the perspective of strategic communication as a basic function of statecraft for the understanding of actors and audiences, and the integration of policies, actions, and words across the government in a coherent way so that strategic communication is used as a means of countering hybrid warfare threats.

Under this frame, hybrid warfare will be defined in the beginning, followed by an analysis of the theory of strategic communication to explore the utility and extent to which it can be applied as a means of countering the hybrid warfare threats.

## **2 Definition of Hybrid Warfare**

Hybrid warfare is a type of a war in which all available resources of a state or a nonstate actor are used with a combination of conventional, unconventional (unorthodox), and political means. Specifically, the term “hybrid” has been used to describe a wide array of measures, means, and techniques including, but not limited to: disinformation; cyberattacks; facilitated migration; espionage; manipulation of international law; threats of force (by both irregular armed groups and conventional forces); political subversion; sabotage; terrorism; economic pressure; and energy dependency [12]. These multifaceted activities may be conducted by separate units or even by the same unit and are operated and regularly directed and coordinated

within the main battlefield in order to achieve synergistic results [13]. Taking into consideration the above frame, hybrid threats can also be created by a state actor using a proxy force. A proxy force sponsored by a major power can generate hybrid threats readily using advanced military capabilities provided by the sponsor [14]. According to Hoffman: “hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics, terrorist acts, including indiscriminate violence and coercion, and criminal disorder” [15]. Hoffman later expanded this definition to reflect hybrid war as being, “sophisticated campaigns that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perception and international opinion” [16]. He also, points out that: “In hybrid warfare, each adversary uses simultaneously and on the same battlefield a tailored mix of conventional weapons, unconventional tactics, and terrorist and criminal actions to achieve its political objectives” [17].

Russia’s actions in Ukraine in 2014 intensified interest in the concept of hybrid warfare.

The Russian doctrine of hybrid warfare as expressed—through an article in 2013 in the Russian Newspaper *Military Industrial Courier*—by the current Chief of the Russian General Staff and Deputy Minister of Defense General Valery Gerasimov, stresses that “civilian means achieve better military or political results than military means” [18]. In particular, Russian techniques included the traditional combination of conventional and irregular combat operations, but also the support and sponsorship of political protests, economic coercion, cyber operations, and, in particular, an intense disinformation campaign. According to General Valery Gerasimov, this new generation of warfare includes the following elements: [19]

- Military action is started during peacetime (without declaring war).
- Noncontact clashes between highly maneuverable specialized groups of combatants.
- Annihilation of the enemy’s military and economic power by quick and precise strikes on strategic military and civilian infrastructure.
- Massive use of high-precision weapons and special operations, robotics, and technologically new weapons.
- Use of armed civilians.
- Simultaneous strikes on the enemy’s units and facilities throughout all of its territory.
- Simultaneous battles on land, air, sea, and in the information space.
- Use of asymmetrical and indirect methods.
- Management of combatants in a unified information system.

NATO, in trying to contextualize the events occurring in Ukraine presented it as being, the use of asymmetrical tactics to probe for and exploit weaknesses via nonmilitary means such as political, informational, and economic intimidation and manipulation and are backed by the threat of conventional and unconventional military means.



Especially, NATO defines hybrid threats as a “type of threat that combines conventional, irregular, and asymmetric activities in time and space” [20]. This provides the essence of something produced by the synergy of different measures but used alone it is too broad.

This perspective of hybrid war establishes an environment that is complex, rapidly changing and nonlinear in character. In this complex environment, the methods employed by a hybrid actor are “the use of military and nonmilitary tools in an integrated campaign, designed to achieve surprise, seize the initiative, and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information; electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure” [21]. In this vein, we can conclude that hybrid threats are characterized by the following actions [22]:

- Are coordinated and synchronized across a wide range of means
- Deliberately target democratic states’ and institutions’ systemic vulnerabilities
- Use a wide range of means
- Exploit the threshold of detection and attribution as well as the border between war and peace
- Aim to influence different forms of decision-making at the local (regional), state, or institutional level
- Favor and/or gain the agent’s strategic goals while undermining and/or hurting the target

Finally, the central theme of this new form of warfare, is the blurring of the boundaries between war and peace between those involved in the conduct of a hybrid conflict (regular and irregular forces or terrorists, criminals, and other nonaligned actors), that see an opportunity to achieve their own goals such as the destabilization of the government or abets the insurgent or irregular warrior by providing resources, or by undermining the host state and its legitimacy [23].

In summary, hybrid warfare is characterized by a hybrid mix of conventional and asymmetric tactics, decentralized planning and execution, with the participation of nonstate actors and the use of both simple and complex technologies in an innovative way [24].

Furthermore, hybrid warfare involves the synchronized use of multiple instruments of power against targeted vulnerabilities of the adversary across the entire spectrum of society’s functions, aiming at effects resulting from the sum of the combined use of the various instruments of power [23]. Finally, hybrid warfare is asymmetrical in texture, employing a variety of power tools in multiple dimensions and levels of escalation simultaneously in a synchronized pattern, emphasizing creativity, unpredictability, and unaccountability, and primarily targeting the cognitive underpinnings of War [23].

### 3 Definition of Strategic Communication

An effective communication response to a hybrid threat or crisis requires effective coordination and the use of all the resources of a state's national power. That is, it requires that a state's diplomatic, intelligence, military, and financial resources be effectively combined to meet the communications objectives of the crisis management team [25].

Strategic communication is approached as a process aimed at understanding key audiences and ensuring their participation and support through informational and psychological operations, public affairs, and public diplomacy [26].

In the implementation of strategic communication, the emphasis goes to the way each organization communicates during the realization of its aims and how it works as a societal structure to promote its mission. The nature and the target of strategic communication play an important role when dealing with a crisis, because while the organizational communication in the broad meaning examines the communication procedure and how people interact in complex organizational situations (interpersonal, collective, digital), strategic communication focuses on the way the organization will represent itself through targeted actions and initiatives of its personnel [27].

According to Richard Halloran [28], strategic communication is a method of persuasion to make others accept ideas, actions or a situation. In other words, it is the mean that an actor has and uses to convince friends and allies to support or to stay neutral, and to adversaries in order they understand that he has the power to dominate on them. It pointed out also, that strategic communication is viewed through the lenses of exercising persuasion in the citizens of a country, in order to support the choices that the political leadership makes, and to that end, build national consent as far as it concerns national goals. Therefore, during the communication confrontation of a crisis, strategic communication is able to exert effective influence in the target—audience, to achieve required perceptions and behaviors, to influence the attitude—stance of the stakeholders involved in a crisis, to moderate or change negative or hostile views of public opinion, allowing the interested actor to acquire the desirable legitimacy to materialize its strategy [27].

In the case of military operations, strategic communication is a continuous function that occurs throughout the whole spectrum of military operations. Joint force strategically communicates with friends and rivals. Similarly, it strategically communicates with the public, population groups, governments, and other organizations, in the framework of conflicts, competition, and cooperation, while it also includes communication with domestic audiences [29].

Furthermore, as Dr. Harlan K. Ullman points out hybrid war is like old wine in a new bottle, in which technology and globalization have transformed aspects of war in the twenty-first century. Limits in military achievements, economic interdependency, and cyber technology are just a few examples of how the new bottle has taken another contour [30].

Moving further, the boundaries between the different aspects of strategic communication are blurred and this is reflected as to whether strategic communication should be considered as “communication of strategy or communication as a strategy.” In the first case, the role of communication is limited to the implementation of a strategy, in a primarily secondary role. The strategy makers decide for it and then, activities are coordinated, such as press conferences and information campaigns, which operate as a reactive measure in times of crisis.

In this context, the coordination capacity of the policymakers focuses on the process of getting the right message from the target audiences and addressing the factors that can weaken the strength of this message. However, this perspective overlooks the ways in which each government actor communicates, by engaging in activities involving separate actions, words, and policies. In relation to the definition of the term “strategic communication,” it should be noted that, despite the fact that strategic communication is widely used in international relations, the academics and professionals of strategic communication do not clearly define its content and the way it can be used.

In particular, from the perspective of international relations, strategic communication is approached as a process aiming at enabling publics to understand, and ensure their participation and support, through information operations, actions related to public affairs and public diplomacy ([31], Paxviii).

Approaching this procedure, thus, seeks to ensure consistency between the messages transmitted and the objectives pursued, in order to avoid communication overlaps or inefficiencies. In order to achieve this consistency, a strategic communication program requires the participation of all of the above components, either at a strategic or at an operational level [31]. Strategic communication is also approached as a capability or an activity supported by certain capabilities ([32], p. 22).

Specifically, in line with this approach, in order for an actor to communicate strategically, it should have the ability to develop a communication plan, synchronize all the functional parts involved in the implementation of the strategic communication program, and, finally, the ability to use specific channels of communication to transmit its messages [32].

In addition, strategic communication is approached as a means of achieving results [31]. More specifically, according to this approach, strategic communication is the means for a body to inform its stakeholders and the public and to exercise influence on them over specific issues. Lastly, strategic communication is viewed as an art form [31]. According to this approach, strategic communication seeks to control the communication environment of an international actor with the aim of shaping the attitudes and behavior of its stakeholders and public.

In 2009, the US Department of Defense in a Strategic Communication Report pointed out that strategic communication should be approached as a process, not a set of capabilities or distinct organizational activities. In this respect, it was stressed that strategic communication “is the process of integrating the stakeholders’ issues, as well as of those that affect the public, in the policy development and the implementation planning of operations to be executed at each hierarchical/functional level” [33].

Therefore, the strategic communication process can result in a more efficient harmonization of government activity to lead and coordinate the decision-making process in a manner favorable to national interests. It should be supported as a guiding principle at all government sectors and levels in order to be effectively implemented. This principle fits into the articulation of strategic communication as a philosophy or mindset. The implementation of strategic communication as a process can function as a binding film between strategy and action, integrating efforts across the government and favoring the unity of effort toward the common strategic objectives.

Such an approach would maximize the use of available resources and reduce the risk of failure. This requires a strategic culture of communications absorbed at all levels of government that looks at foreign policy through the “lens” of communication, identifying relevant audiences and understanding how they form views and make decisions. There will inevitably be specific competence requirements, such as assessment and analysis, planning and implementation of transnational activities, such as media management, public opinion management of stakeholders, marketing, and the level of engagement of actors.

It is understandable that as much as strategic communication is stronger, the fewer procedures are required. In practice, these two approaches—communication at the core of the strategy’s development, or subsequently in the implementation phase—are not mutually exclusive. They are often incorporated in varying degrees, either deliberately or as a feature of the way that governments operate. This is reflected in the balance that governments need to find between the expansion of all specialized communication capabilities and the encouragement of a strategic communication culture, which is indispensable in every section, policy, and strategy [34].

## **4 Strategic Communication as a Mean for Countering the Hybrid Threats**

According to Sun Tzu, the first attack a general will launch is against the moral of the enemy. Moreover, Sun Tzu writes down: «In times of war, adaptability and flexibility are needed», concepts strongly related with hybrid threats almost 2500 years before. He continues in his masterpiece “The art of war”: “the greatest achievement is not to fight and win all of your battles, but to break the will of the enemy to resist, without a battle” [35].

A smart leader overwhelms the enemy without a fight. He conquers his cities without besieging them. He wins his empire without long-lasting operations in the battle field. He invades to his terrain against its governor and his triumph is ultimate without losing a single man [35].

The shift of the conflict from the physical to the information environment, as a theory, is based on the idea that the “War for Hearts and Minds” is an integral,

permanent, and decisive existing element in today's conflicts, the implementation of which is carried out after thorough planning by the participants. The impact of public opinion on military actions creates the need for those involved to incorporate communication as one of the key elements in the planning and execution of any operation. However, as the media environment becomes increasingly complex, results can be pursued and achieved even without an actual—physical conflict [36]. Modern conflict can range from political confrontation to physical confrontation. The boundaries between peace and war have blurred and the information environment acts as a battlefield, where rival narratives clash to prevail over one another, to guide and shape public opinion. Even actual conflicts or proxy wars can be exploited as strategic communication platforms, serving the interests of third parties [36]. In the context of hybrid warfare, the focus of the strategic competition is the so-called “information battles,” in which information is turned into a weapon, and a struggle for the predominance of one's “truth” becomes a struggle. Under this perspective, hybrid threats have the malign intent of manipulating the political decision-making processes of a targeted nation by influencing the behaviors and attitudes of key audiences such as media organizations, the general public, and political leaders [12]. Furthermore, can be considered as information or influence activities. These are actions that influence audience perception and decision-making. Such activities are not limited to the “Information” instrument but involve the combination of different instruments of power, including diplomatic, economic, and military [12]. The smart use of information, through the tailoring of messages, narrative, and persuasion, is able to potentially reach the whole world and provide a dynamic impact on various target audiences. The use of information in a strategic way can exert influence on the stakeholders of a hybrid crisis and a crisis manager wins legitimacy and support from them during the management of the crisis. In this vein, during the management of a hybrid crisis, it is a necessity the delivery of information at the right time and in a coherent manner via the correct message, the suitable and effective communication tools, so that to provide a satisfactory advantage over an opponent, with a massive effect and precision in disrupting and balancing him.

The hybrid warfare is conducted on three interrelated fields of operation. The first is the physical domain, the second is the digital domain, and the third is the cognitive domain. On all three domains, the most hybrid warfare strategies are related to information and communication. The quintessence of all operations is communication and its effective utilization during information and psychological operations. That is, information dominates all fields of operations; therefore, it is of paramount importance to understand the information environment in which hybrid operations are conducted. The information environment represents a set of factors, resources, and processes, which demonstrate the knowledge that has been accumulated and used by a specific society, community, or individual, looking also at ideas and assumptions. There is also the issue of how this knowledge can be obtained, created, expanded, and used. This means that the information environment is a requirement for the survival of individuals and societies and for progress in the development of individuals and societies. That is because information provides an opportunity for necessary exchanges between and among us [37].

In summary, the Information Environment (IE) is a model for understanding how actors and audiences interact, how people see the world around them and consequently make decisions based on the meaning they deduce from it [38]. In this context, during a hybrid operation, a hybrid actor tries to control and influence the information environment of its enemy. Through the control and manipulation of information, a hybrid actor tries to influence the cognitive level of the population and the stakeholders of its opponent. He conducts operations that affect the mind and the emotional level of his audiences through the spread of fear, doubt, and uncertainty about the outcome of the crisis. His objective is to break the morale of the opponent's citizens, to create polarization and controversy so as to shake the citizens' trust in its leadership, and to create social instability and destabilization in the targeted nation.

Taking into consideration the above mention, the author of this article believes that strategic communication is the appropriate tool for the prevention, detection, and reduction or elimination of the consequences of hybrid threats. Since the hybrid information environment is complex and the confrontation of hybrid threats requires the allocation of significant national resources, strategic communication can contribute to the understanding of the information environment. In particular, it helps the managers of hybrid threats or crises to proceed in the human perception assessment and in the shaping of human perception about the situation of a hybrid threat or crisis. Human perception's assessment should be central to the understanding of the dynamics of hybrid threats, the way they are being perceived, interpreted, and attributed to. The analysis should focus on the relevant issues and components of a hybrid threat or crisis: actors (political leaders, civil society, and military), networks (military, economic, cyberspace), and the means (disinformation, cyberattacks, bribery) and understanding how they could exploit vulnerabilities to harm national security interests. The continuous assessment should define the basic regularity lines (of operations, for instance, during an operational planning) and define modifications in standards (operational standards) [29]. In this procedure, strategic communication can ensure the exchange of information, both within and between governments, and the ability to synthesize different types of information and elaborate intelligence. It can put suitable information at the heart of all levels of policy, planning, and implementation, and then, as a fully integrated part of the overall effort, ensure the development of practical, effective strategies that will make a real contribution to the successful management of a hybrid threat or crisis.

Additionally, strategic communication consists the mean of the sensemaking of a hybrid threat or crisis from the managers of a hybrid threat or crisis and also from the stakeholders in a specific way that favors the crisis managers. Sensemaking is the process of social construction that occurs when discrepant cues interrupt individuals' ongoing activity, and involves the retrospective development of plausible meanings that rationalize what people are doing. Central to the development of plausible meanings is the bracketing of cues from the environment, and the interpretation of those cues based on salient frames. Sensemaking is thus about connecting cues and frames to create an account of what is going on [39].

Crises, by their nature, come as a surprise. They often shock a system so radically that responders, at least for a moment, have no clear idea how to respond. From the perspective of sensemaking, understanding of a crisis situation comes from taking action and observing the feedback to that action. Organizations make sense of their environments retrospectively through a sequence of three stages: enactment (action), selection (interpretation), and retention (learning). This process is generally based on interpreting feedback from an organization's environment. If the feedback is positive, more of the same action is warranted. Conversely, negative feedback requires divergent response strategies [40]. Taking into account the above definition, in the case of a hybrid threat or crisis, strategic communication is central to interpreting this feedback and developing a coordinated response.

Furthermore, strategic communication consists of the meaning-making [41] of a hybrid threat or crisis from the managers of a hybrid threat or crisis. Via meaning-making crisis, leaders employ deliberate and concerted moves to influence public perceptions and emotions [42]. In this vein, the managers of a hybrid threat or crisis utilize strategic communication for the framing [43] of the crisis in such a way that highlights positive elements of the crisis and which will exert influence on stakeholders and the citizens so that managers of a hybrid threat or crisis receive legitimacy and support.

Additionally, during the procedure of managing a hybrid threat or crisis, strategic communication is a reliable strategic tool for planning, coordinating, and implementing a crisis communication plan that will cover the following strategic communication goals. It helps in the deconstruction of the rhetoric and the argumentation of hybrid actors (it is the right instrument for dealing directly and effectively with the disinformation campaigns), in the mitigation of disputes and the negative attitude of stakeholders or social groups affected by the crisis, in the mobilization of all institutional and social forces, as well as the alliances of an agency/organization involved in the crisis, in order to support the efforts of the crisis management team to cope with the hybrid threat or crisis and support the procedure of legitimization of the crisis manager's strategy by the audiences who are in their internal and external environment and the wider national and international audiences [44].

Furthermore, strategic communication is the proper mean for the information and education of the stakeholders who are involved in a hybrid crisis as well as the wider population of one hybrid target. During the management of a hybrid threat or crisis, many managers fail to communicate with their audiences because the audience members resist their messages because they contradict adopted habits and ingrained behaviors. Understanding of human perception and behavior should be central to understanding the dynamics of hybrid threats. Through strategic communication, the managers of hybrid threats or crises can understand how their audiences are perceived, interpreted, and attributed in their messages and can produce effective narratives where they will appeal directly or indirectly to targeted audiences using appropriate emotional or logical persuasive appeals designed to elicit desired attitudes and behaviors.

Another field where strategic communication can contribute to managing a hybrid threat or crisis is the area of deterring a hybrid actor. Successful deterrence, in the form of a decision not to pursue intended action, is induced in the mind of the hostile actor, meaning both public and private communications play an important role in shaping the perception. When deciding on a deterrence strategy, one should consider steps to ensure that a hostile actor understands that the pressure imposed is linked to its hybrid activity.

Effective communications are crucial to ensuring this and can reduce the risk of the hostile actor spinning the narrative by portraying the actions as provocative or hostile.

As already mentioned above, strategic communication is a method of persuasion to make others accept ideas, actions, or a situation, and all actions, images, words, and policies, a government takes (or does not take) communicate something. If a government communicates with its audiences strategically via a collective and integrated strategic communication campaign and is guided by a national strategy that has the consensus and the legitimacy of the population, strategic communication can be utilized as a deterrence means of any hybrid actor. The notion of deterrence is based on the core principle of changing the hostile actor's calculus. The goal should be the deterring actor's words and actions leading to a situation where the hostile actor decides not to pursue a particular activity [45]. Via strategic communication, the deterring actor can communicate its strengths, capabilities, and resilience effectively with a message to be seen as coherent and credible and to influence the cognitive and psychological domain of the hybrid actor so that to cancel his purposes. Moreover, as part of resilience-building, strategic communication with one's population is important. It is important to make sure the public is aware of both the threats to national security and the state's preparedness to respond. The same applies to international partners and allies—popular support is a powerful and important tool in democracies. Hostile actors should also have an understanding of a deterring actor's resilience, with the aim of showing that hostility will be futile [45].

## 5 Conclusion

This article consists of an interdisciplinary approach to the communication management of hybrid threats and crises. Specifically, through an interdisciplinary study of International Relations and Communication disciplines, an attempt has been made to approach these disciplines in a multidisciplinary manner in order to identify the concept of hybrid warfare and to present the role that strategic communication plays as a means to counter them. Hybrid warfare is an attractive option for countries seeking to change the status quo, but lacking the power to impose their will by brute force. With the innovative use of new and relatively low-cost tools, they can achieve their goals by taking small steps at a time, but also by achieving the surprise of their opponents with minimal risk. As Frank Hoffman [23] points out,



“Hybrid threats are those covert or illegal activities of nontraditional politicians that fall below the threshold of armed organized violence, including disruption of order, political subversion of governmental or nongovernmental organizations, psychological actions, abuse of legal processes, and financial corruption as part of an integrated plan to achieve strategic advantage.”

Such actions are coordinated, synchronized, and deliberately target the vulnerabilities of democracies and institutions. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution [46].

The hybrid tactics which can be used by an attacker are various forms of sabotage, disruption of communications, and other services including energy supplies. The aggressor may work through or by empowering proxy insurgent groups, or disguising state-to-state aggression behind the mantle of a “humanitarian intervention.” Massive disinformation campaigns designed to control the narrative are an important element of a hybrid campaign [47]. Furthermore, NATO defines hybrid threats as a “type of threat that combines conventional, irregular, and asymmetric activities in time and space.” This provides the essence of something produced by the synergy of different measures but used alone it is too broad [20].

In a combination of the above definitions, some characteristics can be used so that a common understanding can be built concerning this “modus operandi” [48]. Specifically:

- Cyber today is a military domain and in the near future the cognitive domain probably.
- There are no physical borders.
- All actions are coordinated and synchronized across a wide range of means.
- They deliberately target democratic states and institutions systemic vulnerabilities.
- Actors use a wide range of means; they exploit the threshold of detection and attribution as well as the border between war and peace.
- The aim is to influence different forms of decision-making at the local (regional), state, or institutional level, favor and /or gain the agent’s strategic goals while undermining and/or hurting the target.

Until now, in the conventional war, there was a clear distinction between peace and war, but hybrid warfare is a form of war that is in the “gray zone” between peace and war. It is an act of guerilla tactics and means aiming to coerce and to pressure the opponent and to maintain a continuum of war [3].

With the new realities, in the hybrid warfare: [49]

- There is no traditional battlefield (this can be a capital city, a religious site, an airport, a school, a theater, a soccer stadium, etc.).
- The means have fundamentally changed (for example terrorism, piracy, incite social disorder, kidnapping, social media, etc.).

- The strategic aim of the hybrid actor is to terrify the society and to decline the morale of the population of the opponent, so he will subdue the enemy by corrosion in the internal and international field of legitimacy in many domains of the confrontation.

Through the employment of hybrid tactics, the attacker seeks: [50]

- To undermine and destabilize an opponent
- The dominance of an actor in the physical and psychological battlefield through control of information and media
- Exercising influence in order to bend the will of the opponent and to weaken his support from his population and his state services

Under these developments, it is necessary to consider that the weaponization of the communication as a means of hybrid warfare will further deteriorate the worldwide stability and security environment. Particularly, the failure to cope with this threat would definitely increase the conflicts between state and nonstate actors.

In the contemporary complex information environment, a strategic communication campaign aims to create, promote, and maintain a stable image of a country or an organization [51]. It transmits messages, information, and images with a certain scope and serves as both a way and a means to achieve the desired political ends [52]. Especially, in the context of hybrid warfare, information plays a critical role as conflict does not usually escalate into direct armed conflict [53]. The role of nonmilitary means to achieve political and strategic gains has increased, because in the balance among costs and benefits each actor calculates, the use of hard power comes as a following option, considering the destructiveness of the high-tech weapons and the severe economic cost. Within this context, the paper presented how strategic communication as a component of national strategy can help the crisis managers or the decision makers of a government to counter hybrid threats and respond to current and future national security challenges. Specifically, strategic communication is approached as a process aiming at enabling publics to understand and ensure their participation and support, through information operations, actions related to public affairs, and public diplomacy [31]. This approach seeks to ensure consistency between the transmitted messages and the pursued objectives in order to avoid communication overlaps or inefficiencies. In order to achieve this consistency, a strategic communication program requires the participation of all of the above components, either at a strategic or operational level [31].

Therefore, the strategic communication process can result in a more efficient harmonization of government activity to lead and coordinate the decision-making process in a manner favorable to national interests. It should be supported as a guiding principle at all government sectors and levels in order to be effectively implemented. This principle fits into the articulation of Strategic Communication as a philosophy or mindset. This requires the exchange of information, both within, and between governments and the ability to synthesize different types of information and elaborated intelligence. The communication must be governed by the whole of government approach. It should be, therefore, collective and comprehensive. Based

on a comprehensive understanding and continuous assessment of the information environment, governments should have a clear understanding of means available in order to reach audiences. This could be anything, from financial sanctions to a change in stance through the use of military force. All these should be incorporated and used coherently to achieve the desired strategic impacts and results. Actions taken to counter threats/hybrid threats should be guided by a strategy. The reflection on strategic communication must be at the core of the development and implementation of the strategy from the outset, and this process should be supported by the availability of appropriate resources and highly specialized personnel. National strategy should have a broad consensus for the population to support it and be supported from the top by the political leadership. This includes the formulation of the strategic position that a nation wants to take, and the way it would be structured throughout the government, engaging ministries, such as those responsible for culture, education, and home affairs. Such an approach ensures that any “story” (or national narration/narrative) that the government wants to communicate is authorized at all levels, coherent and consistent. National authorities should have structures that are flexible, decentralized, and adaptable, capable for preparation, agility, and response. The nature of threats/hybrid threats means that there are no identified handbooks that can be followed. Adversaries will continue to develop, test, and implement measures targeted at vulnerabilities. Fostering a culture of strategic communication in all government agencies will allow a nation to maintain its initiative to act [34]. The attribution of hybrid threats to an adversary is a political effort based on the public’s confidence, so reliability should be protected as a vital resource. Any governmental action, which impairs public’s confidence, will reduce the actions available for preparedness and response to hybrid threats. In any case, it should be understood that, even if there is no obvious link between the particular area of responsibility of each of the parties involved and national security, their actions can weaken national resilience [29].

## References

1. Śliwa, Z., Veebel, V., Lebrun, M.: Russian ambitions and hybrid modes of warfare. *Estonian J. Military Stud. Sõjateadlane*. 7, 86–108 (2018)
2. <https://www.nationalgeographic.org/encyclopedia/rainbow/#:~:text=When%20sunlight%20hits%20a%20rain,is%20separated%2C%20producing%20a%20rainbow> (last access 26.01.2023)
3. Julio, M.-C.: Hybrid Warfare: NATO’s New Strategic Challenge? 166 DSC 15 E bis, p. 3. NATO Parliamentary Assembly (2015)
4. García, J.P.V., Quirós, C.T., Soria, J.B.: Strategic Communications as a Key Factor in Countering Hybrid Threats. European Parliamentary Research Service, Brussels (2021)
5. Tatham, S.: Strategic communication: A primer. *ARAG Special Ser. Defence Acad. U. K.* 18(28), 3 (2008)
6. Robert, K.: *The Jungle Grows Back: America and our Imperiled World*. Alfred A. Knopf, Penguin Random House LLC, New York (2018)
7. Survey Global University Alliance and NATO with title: Agile Multi-Domain Socio-Technical Enterprises in Hybrid Operations. For more see: <https://www.globaluniversityalliance.org/research/enterprises-in-hybrid-operations/> (last access 27/1/2023)

8. Mazarr, M.J.: *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Monographs, Books, and Publications, US Army War College Press (2015)
9. General Joseph L. Votel, statement before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities (March 18, 2015)
10. Barno, D., Benschel, N.: *Fighting and Winning in the 'Gray Zone,' War on the Rocks*, May 19, 2015. For more see: <https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/> (last access 31/1/2023)
11. See: <https://www.csis.org/programs/gray-zone-project> (last access 31/1/2023)
12. Sean Aday, Māris Andžāns, Una Bērziņa-Čerenkova, Francesca Granelli, John-Paul Gravelines, Mills Hills, Miranda Holmstrom, Adam Klus, Irene Martinez-Sanchez, Mariita Mattiisen, Holger Molder, Yeganeh Morakabati, James Pamment, Aurel Sari, Vladimir Sazonov, Gregory Simons, Jonathan Terra, *Hybrid Threats. A Strategic Communications Perspective*, NATO Strategic Communications Centre of Excellence (NATO StratCom COE), Riga, 2019
13. Miller, M.: *Hybrid Warfare: Preparing for Future Conflict*, p. 7. Air War College, Air University, Maxwell AFB, AL (2015)
14. Mumford, A.: Proxy warfare and the future of conflict. *RUSI J.* **158**(2) (2013)
15. Celso, A.N.: Superpower hybrid Warfare in Syria. *Marine Corps Gazette.* **9**(2), 92–116 (2019)
16. Graham, F.: The mouse, the tank and the competitive market: A new view of hybrid war. In: Özel, Y., Inaltekin, E. (eds.) *Shifting Paradigm of War: Hybrid Warfare*. Turkish National Defense University Army War College, Istanbul (2017)
17. Frank, H.: *On Not-So-New Warfare: Political Warfare vs. Hybrid Threats, War on the Rocks*, July 28, 2014
18. Coalson, R.: *Top Russian General Lays Bare Putin's Plan for Ukraine,* The World Post, September 2, 2014
19. Andis, K.: *Hybrid War – A New Security Challenge for Europe*. Centre for East European Policy Studies, Latvia (2015)
20. NATO Standardization Office (NSO): AAP-6, NATO Glossary of Terms and Definitions, p. 62 (2018)
21. Wither, J.K.: Making sense of hybrid warfare. *Connections. Q. J.* **15**(2), 73–87 (2016) and *Complex crises call for adaptable and durable capabilities. Mil. Balance.* **115**(1), 5 (2015)
22. Aday, S., Andžāns, M., Bērziņa-Čerenkova, U., Granelli, F., Gravelines, J.-P., Hills, M., Holmstrom, M., Klus, A., Martinez-Sanchez, I., Mattiisen, M., Molder, H., Morakabati, Y., Pamment, J., Sari, A., Sazonov, V., Simons, G., Terra, J.: *Hybrid Threats. A Strategic Communications Perspective*, p. 10. NATO Strategic Communications Centre of Excellence (NATO StratCom COE), Riga, 2019 and Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue, *Addressing Hybrid Threats* (Swedish Defence University, Center for Asymmetric Threat Studies, Hybrid CoE) (2018)
23. Hoffman, F.G.: *Conflict in the 21 Century: The rise of Hybrid Wars*. Potomac Institute for Policy Studies, Arlington (2007)
24. General J.T.: Conway, USMC, Admiral Gary Roughead, USN and Admiral Thad W. Allen, USCG, *A Cooperative Strategy for Maritime Security*, Washington, D.C., October 2007. Conway, James T.; Roughead, Gary; and Allen, Thad W. (2008) "A Cooperative Strategy for 21st Century Seapower", *Naval War College Review*, Vol. 61, No. 1, Article 3, 2008
25. Balomenos, K.: *Strategic Communication and Terrorism: Management of Terrorist Crises*. Poiotita Publications, Athens (2017)
26. Farwell, J.P.: *Persuasion and Power: the Art of Strategic Communication*. Georgetown University Press, Washington, DC (2012) p. xv
27. Balomenos, K.: *PhD thesis: Strategic Communication as a Strategic Tool and soft Power Factor in Resolving International and Business Crises*, pp. 19–20. University of Piraeus (2016)
28. Richard, H.: *Strategic Communication*, pp. 4–14. *Parameters* (2007). Available at <https://www.strategicstudiesinstitute.army.mil/pubs/parameters/Articles/07autumn/halloran.pdf.1> (last access 14.03.22)

29. Balomenos, K.P.: Turkey's Strategic Communication Campaign in Operation "Peace Spring", pp. 11–14. Research Institute for European and American Studies (RIEAS) and Libya Institute for Advanced Studies (LIAS), Athens (2020)
30. Ullman, H.K.: Hybrid War: Old Wine a New Bottle? Huffington Post. Retrieved October 9, 2018, from [https://www.huffingtonpost.com/dr-harlan-k-ullman/hybrid-war-old-wine-in-a-b\\_6832628.html?guccounter=1](https://www.huffingtonpost.com/dr-harlan-k-ullman/hybrid-war-old-wine-in-a-b_6832628.html?guccounter=1) (last access 16.02.23) (2015)
31. Farwell, J.P.: *Persuasion and Power: The art of Strategic Communication*, p. xv. Georgetown University Press, Washington, DC (2012); Balomenos, K.: PhD thesis: *Strategic Communication as a Strategic Tool and Soft Power Factor in Resolving International and Business Crises*, pp. 184–185. University of Piraeus (2016)
32. Paul, C.: *Strategic Communication: Origins, Concepts, and Current Debates*, pp. 22–23. Praeger an Imprint of ABC -CLO, LLC, USA (2011); Balomenos, K.: PhD thesis: *Strategic Communication as a Strategic Tool and Soft Power Factor in Resolving International and Business Crises*, pp. 184–185. University of Piraeus (2016)
33. US Department of Defense: *Report on Strategic Communication*, p. 1. Washington, DC. (2009). <http://www.au.af.mil/au/awc/awcgate/dod/dodreport/strategic/communication/11fee10.pdf>; Balomenos, K.: PhD thesis: *Strategic Communication as a Strategic Tool and Soft Power Factor in Resolving International and Business Crises*, pp. 184–185. University of Piraeus (2016)
34. NATO StratCom Centre of Excellence: *A Strategic Communications Perspective*, The Strategic Communications Mindset, p. 21
35. Tzu, S.: *The Art of War*, 2nd edn. Communication Publications, Athens (2002)
36. Nikezis, E.: *Redefining the battlefield: From the physical to the information environment*. In: *Transcripts of Seminar: Applied and Holistic Management of Hybrid Threats and Crises*. Hellenic Ministry of National Defence – General Directorate for National Defence Policy and International Relations (DGPEADS) (2020)
37. Brikše, I.: *The Information Environment: Theoretical Approaches and Explanations*. Semantic Scholar (2006)
38. U.S. Joint Chiefs of Staff: *Joint Publication 3–13: Information Operations, Incorporating Change 1*, pp. 1–2. Washington, DC (2014)
39. Maitlis, S., Sonenshein, S.: *Sense-making in crisis and change: Inspiration and insights from Weick*. *J. Manag. Stud.* **47**, 3 (2010)
40. Sellnow, T.L., Seeger, M.W.: *Theorizing Crisis Communication*. Wiley-Blackwell (2013)
41. *Meaning-making is the process of how people construe, understand, or make sense of life events, relationships, and the self*
42. Arjen, B., Paul't, H., Eric, S., Bengt, S.: *The Politics of Crisis Management Public Leadership under Pressure*. Cambridge University Press, New York/Melbourne/Madrid/Cape Town/Singapore/São Paulo (2005)
43. *The process of framing involves cutting out a few elements of a perceived reality and "assembling" them into a new narrative, which highlights specific connections between them, in order to promote a particular interpretation. In particular, the way an issue is framed by the managers of a hybrid threat or crisis can determine how public opinion will observe, understand and record the issue in question, as well as how it will evaluate and act/react to it. For more see: Entman Robert M.: Framing: Toward Clarification of a Fractured Paradigm, Communication, 43:4, (1993)*
44. Balomenos, K.P.: *Speak or not to Speak with One Voice during a Crisis?* In: *NRDC-HERALD –The magazine of NATO Rapid Deployable Corps-Greece*, Issue 19, (2022)
45. Keršanskas, V.: *DETERRENCE: proposing a more strategic approach to countering hybrid threats*, The European Centre of Excellence for Countering Hybrid Threats Paper 2, March 2020
46. <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>, The European Centre of Excellence for Countering Hybrid Threats
47. *Research Global University Alliance & NATO with Title: Agile Multi-Domain Socio-Technical Enterprises in Hybrid Operations. For more info follow: <https://>*

- [www.globaluniversityalliance.org/research/enterprises-in-hybrid-operations/](http://www.globaluniversityalliance.org/research/enterprises-in-hybrid-operations/) (last access 20/8/21)
48. Šliwa, Z., Veebel, V., Lebrun, M.: Russian ambitions and hybrid modes of Warfare. *Estonian J. Mil. Stud.* Sõjateadlane. 7, 86–108 (2018)
  49. Andreas, J., Guillaume, L.: NATO's Hybrid Flanks – Handling Unconventional Warfare in the South and the East NATO Research Paper, No. 112, p. 3, Brussels (2015)
  50. Andis, K.: Hybrid War – A New Security Challenge for Europe Centre for East European Policy Studies. Latvian Presidency of the Council of the European Union (2015)
  51. UK Ministry of Defence (MOD) Crown: Joint Doctrine Note 2/19 Defence Strategic Communication. DCDC Ministry of Defence Shrivenham, Swindon, Wiltshire (2019)
  52. Yarger, H.R.: Strategic Theory for the 21st Century: the Little Book on Big Strategy. Strategic Studies Institute, Carlisle (2006)
  53. UK Ministry of Defence (MOD) Crown: Joint Concept Note 2/18 Information Advantage. DCDC Ministry of Defence Shrivenham, Swindon, Wiltshire (2018)

## **Sources**

### ***International Bibliography***

- Arjen, B., Paul't, H., Eric, S., Bengt, S.: *The Politics of Crisis Management Public Leadership under Pressure*. Cambridge University Press, New York/Melbourne/Madrid/Cape Town/Singapore/São Paulo (2005)
- Balomenos, K.: *Strategic Communication and Terrorism: Management of Terrorist Crises*. Poiotita Publications, Athens (2017)
- Balomenos, K.P.: PhD Thesis: *Strategic Communication as a Strategic Tool and Soft Power Factor in Resolving International and Business Crises*. University of Piraeus (2016)
- Balomenos, K.P.: *Turkey's Strategic Communication Campaign in Operation "Peace Spring"*. Research Institute for European and American Studies (RIEAS) and Libya Institute for Advanced Studies (LIAS), Athens (2020)
- Brikše, I.: *The Information Environment: Theoretical Approaches and Explanations*. Semantic Scholar (2006)
- Farwell, J.P.: *Persuasion and Power: the art of Strategic Communication*. Georgetown University Press, Washington, DC (2012)
- Graham, F.: *The mouse, the tank and the competitive market: A new view of hybrid war*. In: Özel, Y., Inaltekin, E. (eds.) *Shifting Paradigm of War: Hybrid Warfare*. Turkish National Defense University Army War College, Istanbul (2017)
- Freeman, E.R.: *Strategic Management: a Stakeholder Approach*. Pitman, Boston (1984)
- García, J.P.V., Quirós, C.T., Soria, J.B.: *Strategic Communications as a Key Factor in Countering Hybrid Threats*. European Parliamentary Research Service, Brussels (2021)
- Heath, R.L.: *Encyclopedia of Public Relations*. Sage publications, USA (2005)
- Derina, H., Ansgar, Z.: *The Routledge Handbook of Strategic Communication*. Routledge, New York/London (2015)

- Robert, K.: *The Jungle Grows Back: America and our Imperiled World*. Alfred A. Knopf, Penguin Random House LLC, New York (2018)
- Walter, L.: *Public Opinion*. Transaction Publishers, USA, London (1991)
- Mazarr, M.J.: *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. Monographs, Books, and Publications, US Army War College Press (2015)
- Miller, M.: *Hybrid Warfare: Preparing for Future Conflict*. Air War College, Air University, Maxwell AFB, AL (2015)
- Julio, M.-C.: *Hybrid Warfare: NATO's New Strategic Challenge?* 166 DSC 15 E bis. NATO Parliamentary Assembly (2015)
- NATO StratCom CoE, *Daesh Propaganda, before and after its Collapse Countering Violent Extremism*, June 2019
- NATO StratCom CoE: *Improving NATO Strategic Communications Terminology*, June 2019
- Thomas, N.: *The Weaponization of Social Media & Characteristics of Contemporary Conflicts*. Royal Danish Defence College (2015)
- Paul, C.: *Strategic Communication: Origins, Concepts, and Current Debates*. Praeger an Imprint of ABC-CLO, LLC, USA (2011)
- UK Ministry of Defence (MOD) Crown: *Joint Concept Note 2/18 Information Advantage*. DCDC Ministry of Defence Shrivenham, Swindon, Wiltshire (2018)
- Anders, R.G.: *Paper: Definitions of strategic political communication*. Norwegian Institute of International Affairs (2005)
- UK Ministry of Defence (MOD) Crown: *Joint Doctrine Note 2/19 Defence Strategic Communication*. DCDC Ministry of Defence Shrivenham, Swindon, Wiltshire (2019)
- USA Department of Defence: *Strategic Communication Joint Integrating Concept, Version 1*, Oct 2009
- US Department of Defense: *Report on Strategic Communication*, Washington, DC, December 2009
- U.S. Joint Chiefs of Staff: *Joint Publication 3-13: Information Operations, incorporating change 1*, (Washington DC (2014)
- Aday, S., Andžāns, M., Bērziņa-Čerenkova, U., Granelli, F., Gravelines, J.-P., Hills, M., Holmstrom, M., Klus, A., Martinez-Sanchez, I., Mattiisen, M., Molder, H., Morakabati, Y., Pamment, J., Sari, A., Sazonov, V., Simons, G., Terra, J.: *Hybrid Threats. A Strategic Communications Perspective*. NATO Strategic Communications Centre of Excellence (NATO StratCom COE), Riga (2019)
- Sellnow, T.L., Seeger, M.W.: *Theorizing Crisis Communication*. Wiley-Blackwell (2013)
- Tzu, S.: *The Art of War*, 2nd edn. Communication Publications, Athens (2002)
- Transcripts of Seminar: *Applied and Holistic Management of Hybrid Threats and Crises*, Hellenic Ministry of National Defence – General Directorate for National Defence Policy and International Relations (DGPEADS) (2020)
- Yarger, H.R.: *Strategic Theory for the 21st Century: the Little Book on Big Strategy*. Strategic Studies Institute, Carlisle (2006)

## Articles

- Mumford, A.: Proxy warfare and the future of conflict. *RUSI J.* **158**(2) (2013)
- Celso, A.N.: Superpower hybrid Warfare in Syria. *Marine Corps Gazette.* **9**(2), 92–116 (2019)
- Balomenos, K.P.: Speak or not to Speak with One Voice during a Crisis? In: NRDC-HERALD –The magazine of NATO Rapid Deployable Corps-Greece, Issue. **19** (2022)
- Coombs, T.W.: Impact of past crises on current crisis communication: insights from situational crisis communication theory. *Business Commun.* **41**(3) (2004)
- Tom, C., Per, L., Rykkja, L.H.: How to cope with a Terrorist Attack? A challenge for the political and administrative leadership. In: European Commission Coordinating for Cohesion in the Public Sector, 6th edn, (2012)
- Entman, R.M.: Framing: Toward Clarification of a Fractured Paradigm. *Communication.* **43**(4) (1993)
- Andreas, J., Guillaume, L.: NATO's Hybrid Flanks – Handling Unconventional Warfare in the South and the East NATO Research Paper, No. 112, Brussels (2015)
- Andis, K.: Hybrid War – A New Security Challenge for Europe. Centre for East European Policy Studies, Latvia (2015)
- Coalson, R.: Top Russian General Lays Bare Putin's Plan for Ukraine," *The World Post*, September 2, 2014
- David, G.C., Binnendijk: The Power to Coerce Countering Adversaries Without Going to War. *Rand* (2016)
- Conway, J.T., Roughead, G., Allen, T.W.: A Cooperative Strategy for 21st Century Seapower. *Naval War College Rev.* **61**(1), 3 (2008)
- Bruce, G.: Public Diplomacy and Strategic Communication, Cultures, Firewalls and Imported Norms. George Washington University and Georgetown University, Washington, DC (2015)
- Keršanskas, V.: DETERRENCE: proposing a more strategic approach to countering hybrid threats, The European Centre of Excellence for Countering Hybrid Threats Paper 2, March 2020
- Maitlis, S., Sonenshein, S.: Sense-making in crisis and change: Inspiration and insights from Weick. *J. Manag. Stud.* **47**, 3 (2010)
- NATO Standardization Office (NSO): AAP-6, NATO Glossary of Terms and Definitions (2018 edition), 62
- Šliwa, Z., Veebel, V., Lebrun, M.: Russian Ambitions and Hybrid Modes of Warfare. *Estonian J. Mil. Stud. Sõjateadlane, Sõjateadlane* (2018)
- Tatham, S.: Strategic communication: A primer. *ARAG Special Ser. Defence Acad. U. K.* **18**(28), 3 (2008)
- Wither, J.K.: Making sense of hybrid warfare. *Connections. Q. J.* **15**(2), 73–87 (2016) and Complex crises call for adaptable and durable capabilities. *Mil. Balance.* **115**(1), 5 (2015)



## **Websites**

[https://www.nationalgeographic.org/encyclopedia/rainbow/#:~:text=When%20sun  
light%20hits%20a%20rain,is%20separated%2C%20producing%20a%20rainbow](https://www.nationalgeographic.org/encyclopedia/rainbow/#:~:text=When%20sun%20light%20hits%20a%20rain,is%20separated%2C%20producing%20a%20rainbow)  
[https://www.globaluniversityalliance.org/research/enterprises-in-hybrid-  
operations/](https://www.globaluniversityalliance.org/research/enterprises-in-hybrid-operations/)  
<https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/>  
<https://www.csis.org/programs/gray-zone-project>  
[https://www.strategicstudiesinstitute.army.mil/pubs/parameters/Articles/07autumn/  
halloran.pdf.1](https://www.strategicstudiesinstitute.army.mil/pubs/parameters/Articles/07autumn/halloran.pdf.1)  
[https://www.huffingtonpost.com/dr-harlan-k-ullman/hybrid-war-old-wine-in-a-  
\\_b\\_6832628.html?guccounter=1](https://www.huffingtonpost.com/dr-harlan-k-ullman/hybrid-war-old-wine-in-a-_b_6832628.html?guccounter=1)  
<https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>  
[https://www.globaluniversityalliance.org/research/enterprises-in-hybrid-  
operations/](https://www.globaluniversityalliance.org/research/enterprises-in-hybrid-operations/)

# The Integrated Approach in Countering Contemporary Security and Defence Threats



Fotini Bellou

## 1 Introduction

Current security threats touching also upon the realm of defence have become increasingly ambiguous, composite and complex. A growing propensity is observed in which state or not state actors are engaged in hostile activities against a state and its society by using a number of methods and instruments and often times a combination of them, in order to destabilize or distract segments of sovereignty, or the decision-making process of a state. These activities, which can also lead to conflicts, involve a combination of conventional and asymmetric practices, taking the form of a composite nexus of ‘actors, narratives, tactics and technologies’, whilst at the same time this nexus may interact at local, national or international level ([28]: 49).

By looking at the evolution of the comprehensive approach in managing international crises, this chapter aims to establish that such an approach, if adjusted at the national level in the form of an integrated approach (for some governments, the whole of government approach), can serve better a state’s effort to counter contemporary hybrid threats and hybrid warfare. As will be shown, hybrid warfare and threats target the victimized state’s vulnerabilities, intertwining military, civilian or societal aspects of governance. Recent experience from post-conflict international stabilization and peacebuilding operations has offered analytical and practical tools through the prism of a comprehensive approach in managing crises. This approach started to be fashioned primarily since the international peacebuilding/stabilization involvement in Afghanistan in 2001 and gained further popularity from scholars and

---

F. Bellou (✉)

Department of International and European Studies, University of Macedonia, Thessaloniki, Greece

e-mail: [fbellou@uom.edu.gr](mailto:fbellou@uom.edu.gr)

practitioners so long as it was providing convincing policy responses in countering multifaceted destabilizing conditions in post-conflict environments. An examination of the defining elements of hybrid threats and hybrid warfare indicate that the grey area in which these subversive activities occur striving to disrupt segments of governmental authority as well as societal coherence also seek synchronized and multilayered responses. Precisely for this reason, a comprehensive approach evolves as the most appropriate response against contemporary hybrid threats. For they primarily require counter measures having also a society-centred approach [23], pointing to the ability of state to sustain resilience at all levels of governance.

For this reason, it is important to underline that building resilience at all levels of governance as an endgame resembles to a great degree the effective functioning of a comprehensive approach in crisis management. Indeed, it has evolved as the most appropriate strategy, or organizing principle, in order to address international crises that were involving all segments of governance. For a comprehensive approach in such a context embraces a combination of proactive, inclusive and intersectoral logic upon which all international activities, providing peacebuilding activities, have to be performed. As an organizational structure, it has become also increasingly popular with modern governments in implementing their national high-level strategy, since they have been called to respond to an increasing number of multifaceted and complex hostile actions including hybrid threats and challenges.

In this sense, what was considered a comprehensive approach in the context of international crisis management, involving all different international actors with different cultures and operational logics (military, civilians, international institutions and non-governmental organizations), which had to coordinate their interaction with the local political and societal dynamics of post-conflict spaces, now has taken the form of an integrated approach at the national level. At this level, an integrated approach implies the ability of the state authorities to organize a *unified decision-making body* through which all activities can be integrated and thus coordinated, synchronized and implemented. It is this logic of synchronized coordination that a number of governments and organizations, such as the United States, the United Kingdom, the EU and NATO, have been using the term of integrated approach (and whole of government approach) in recent years in order to describe the organizational principle through which building resilience against hybrid warfare and hybrid threats can be assumed.

The analysis begins with a discussion about the character of hybrid threats as these have been analysed by respective scholarship and institutions. It will be showed that the character of those hybrid activities cut across all levels of analysis: strategic, operational and tactical, by destructing or distorting both military and civilian spaces through conventional or/and asymmetric methods enmeshing also societal issues. The chapter continues by examining the comprehensive approach in managing international crisis through a discussion of the evolution of peacebuilding and stabilization operations in recent years. The chapter concludes with a presentation of the integrated approach that a number of governments and institutions have adopted in recent years as a response to the multifaceted character of hybrid threats primarily viewed under the prism of building state and societal resiliency

by bolstering coherence at all levels of governance. This article advocates that an integrated approach in managing crises, as a number of governments and institutions have already adopted, provides the optimal strategy for states and institutions in order to prevent or deter hybrid threats and attacks.

## 2 The Comprehensive Character of Hybrid Threats

The concepts of hybrid treats and hybrid warfare have received much attention in recent years from scholarly literature, even if hybridity in warfare is not a novelty. Asymmetric wars are neither a novelty [6]. As Ofer Fridman has rightly observed, there is also a difference in meaning of the term hybrid warfare between Western military theorists and Russian strategists [13]. The former focuses primarily on different tactical and operational activities that can be coordinated in the field in order to produce multiple and ‘synergistic effects’ ([13]: 43). The latter adopts a broader interpretation by involving ‘all spheres of public life: politics, economy, social development, culture’ which resembles much of subversion war ([13]: 43).

The Russian interpretation of hybrid warfare also point to the corrosive activities aiming at challenging sociocultural cohesion of the enemy’s population in order to gradually inflict a regime change, whilst the use of force is expected to be reduced at the minimum possible level. For Western interpretations, as these were first depicted by Frank Hoffman, hybrid warfare combines irregular warfare and conventional capabilities, whilst it can involve ‘terrorist acts including indiscriminate violence and coercion and criminal disorder’ ([18]:14). For some military practitioners hybrid threats ‘exploit operational, informational and legal ambiguities and vulnerabilities across all domains’ ([17]: 29).

For a number of scholars, the wars in Iraq and Afghanistan should be considered as contemporary hybrid wars since they involved an amalgam of ethnic or tribal conflict, ideologically driven insurgents and organized crime affiliates, all ready to interact with local warlords and other third actors with little interest to state-building [31]. In hybrid warfare a combination of conventional military operations, insurgency and terrorism may be observed whilst the cyberspace is employed for propaganda, recruitment and communication purposes [31]. Frequently, as Weissmann describes, it ‘blurs the distinct and combatants and both demands and permits all activities necessary to achieve success’ (in [17, 18]: 5) For this reason, it is not surprising to observe a wider exploitation of societal vulnerabilities aiming at distracting social cohesion through a number of distorting ‘soft’ instruments of public diplomacy or influence operations along with the use of ‘full spectrum capabilities, including long distance weapons and Special forces’ ([17, 18]: 5). For this reason, as Mikael Weissmann highlights in the respective conference proceedings, the concept of Key Terrain gains increasing importance, and it might be protected or threatened by ‘increasingly potent Anti-Access Area Denial (A2AD) systems’ ([17]: 5).

Due to different actors involved, in hybrid warfare, namely, state and non-state actors, special operations units, private militias, insurgents and terrorist groups, the international law of war and humanitarian law is sidelined if not instrumentalized in order to serve the actors who use it ([30, 31]: 868). In addition, as Siman points out, hybrid warfare ‘covers the much broader range of influence operations. These seek to undermine trust in the target’s system, through mis/disinformation, coercion, ‘Lawfare’ Threat Finance, “DeepFakes”, assassinations and “Active Measures”, “use of useful idiots”, and criminal activities’ ([32]: 2). In an apparent trend to adopt wider interpretations of hybrid warfare in the aftermath of the wars in Iraq and Afghanistan and following Russia’s first aggression to Ukraine, which culminated with the annexation of Crimea in 2014, scholarly discussion started to involve all those activities that could have possibly have a subversive effect whilst at the same time remain at the level below the declaration of war [38]. These activities ‘short of war’ are considered to be found in the grey zone between war and peace, and thus military responses cannot be justified [19, 40]. The corrosive effect of those practices, or strategies, can prove important so long as they aim at changing the *status quo* [8, 40]. Most importantly, hybrid threats and hybrid warfare can optimize the technological advances but also societal vulnerabilities according to the target space and thus operate in subversive modes by combining different operational domains against which a very demanding military and civilian coordination posture may be required. Indeed, whilst the optimization of different operational domains remains a key aspect of concern in contemporary strategy [22], hybrid warfare has further underlined its importance.

For this reason, a change in strategic thinking is required as to incorporate the interchangeable levels to which hybrid threats can apply whilst at the same time adopt a holistic or comprehensive approach aiming at bolstering those aspects of governance, in multiple domains, that could augment resilience against subversive activities. It is for this reason, that most scholarly discussion correctly points to the importance of states adopting a comprehensive approach in order to counter hybrid threats and warfare [35, 39]. Analysis continues with a discussion on the evolution of the notion of comprehensive approach in managing crises from recent international experience since it provides the most optimal approach in addressing multifaceted, multilayered and composite challenges against state governance.

### **3 The Comprehensive Approach in Crisis Management: A Paradigm to Be Followed**

The shift in post-Cold War international practice, *from traditional peacekeeping operations to multidimensional peace support operations and stabilization missions*, necessitated the international adaptation of both governments and international organizations involved (UN, NATO, OSCE, EU). In the new context, international actors’ (governments and institutions) support in providing certain

segments of governance services became known as post-conflict peacebuilding. International involvement often entailed almost the entire range of the related governance services [5, 11, 12, 41].

As indicated in UN documents, actions and policies implemented in a region in the context of post-conflict peacebuilding operations involve different activities at different stages of progress, a variety of actors, governmental and non-governmental, military and civilian, and even numerous international organizations ([36]: 23). Each external actor used to provide services that in practice set a single stone in the big mosaic governance patterns, or they were inextricably intertwined in a specific sector. Depending on the related know-how functions and capabilities, each international actor was expected to contribute to the provision of services, both tangible and intangible, in order to re-establish the necessary conditions for governance in the region [1].

The aim of these operations had been to strengthen local institutions/authorities in the long term so that they could operate on their own by means of sustainable peace. In other words, the international actors evolved as an integral part of the state's effort to ensure – in practice to build – the right environment for a functioning government that lacked signs of a return to the previous conflict situation. It was important, for the internationals to secure the provision of goods and services to citizens, whilst essential security, development and political inclusiveness requirements are retained [37]. In practice, these 'international actor' services are provided by different international organizations, governments, private companies, non-governmental organizations but also military or police forces as well as civilians operating under governmental decisions or international organizations' mandates, usually on the basis of UN Security Council resolutions.

Peacebuilding operations following the violent dissolution of Yugoslavia and the end of the subsequent wars in the 1990s have offered a real learning opportunity and a valuable familiarization process for the 'international actors' regarding the obligations arising from the difficult task of peacebuilding. Despite the difficulties and initial failures, the operations were carried out almost in their entirety, with no dramatic incidents of engagement in dangerous confrontations (spoilers) and obstruction of peacebuilding work. In other words, they were implemented in a 'permissive environment' where international actors have pursued, and to some extent continue to pursue, the demanding policies required by the peacebuilding toolbox [16]. Of course, such a process does not unfold without problems since certain different actors' perceptions and strategic cultures often make communication and cooperation problematic or even impossible. Nevertheless, internationals offer their different services to support the military, police, civilian, judicial, development, economic and social spheres of operation of the country or region in need. Examples included NATO (IFOR/SFOR, KFOR), the United Nations (UNBiH, UNMIK, UNPREDEP) and the EU (Althea, EULEX, EUForce Concordia, EUPOL Proxima), in Bosnia, Kosovo and North Macedonia. Depending on the complexity of the relevant governance challenges, the international factor focused on specific actions in these areas under the logic of peacebuilding.

The experience of operations in the Western Balkans was often exposed to coherence questions, whilst inconsistencies amongst different actors and often different tactics and cultures delayed or obstructed effective peacebuilding. Therefore, whilst the need for constructive coordination amongst international actors had been documented by both decision-makers and relevant conflict resolution massive literature, there seemed to be no intention of many stakeholders to coordinate under a specific framework for action [25]. Much discussion was focusing on the need for effective civil-military cooperation rather than measuring results [4, 7]. Yet, the expectation of an integrated or comprehensive approach which requires, sustains and engenders unity of purpose has become much more visible and pressing since the mid-2000s through the respective operations of NATO in Afghanistan and the United States in Iraq in 2003 [7, 37].

The unpleasant experience for the 'international actors' (governments, organizations and NGOs) in Afghanistan and of the United States in Iraq, respectively, following the overthrow of the Saddam Hussein regime in 2003, highlighted the need not only for the involvement of an increasing number of international organizations and governments in peacebuilding but also the need for a much more complex and highly demanding response. As also discussed above, multiple hostile actions and terrorist attacks in the field which aimed at disrupting not only the peacebuilding mission but also the international presence itself had to be countered.

Most importantly, it was the practice of weakening the image and practical effectiveness of the internationals through a combination of irregular warfare, taking the form of terrorism, insurgency and criminal activities that Frank Hoffman described also as hybrid warfare (cited in [34]). Their purpose was to demoralize their victims by merging 'different modes and means of war' including information warfare and modern media [34]. Although such modes of actions were not a novelty in warfare, the need for multiple responses cutting across different levels of conduct had become of profound importance [14]. It was the time at which a comprehensive approach started to be advocated as the best possible responses [7, 37].

The Alliance for the first time in the conclusions of the [26] Riga Summit in Latvia, with a reference guide to NATO's mission in Afghanistan referred to the need for a comprehensive approach by the international community in view of modern challenges which would integrate a wide range of civilian and military tools (NATO Riga Summit Declaration, par10. The need for the Alliance to improve the coherent application of its own crisis management tools and to strengthen practical coordination with other relevant international organizations as well as non-governmental organizations, military and civilian actors as well as local actors involved in such operations was also stressed.

Thus, the integrated or holistic approach to crisis management focused in principle on coordinating action by different actors who used their own know-how and capabilities to contribute to a commonly accepted outcome of sustainable peace, although often achieving stability, seen as the absence of conflict, was a more feasible objective. From a strategic point of view, the NATO operation in Afghanistan and the United States' peacebuilding effort in Iraq following the overthrow of the Saddam Hussein regime had 'upgraded', if not reinforced, the

necessity of the integrated approach, namely, not only a coordination amongst different actors working at multiple levels of governance but at the same time being able to conform under a unified single command.

The scope of operations was not just a permissible environment where local authorities named highways in the name of the Alliance and Western leaders (e.g. Balkans) but weak governments very often attacked by local guerrilla groups, fanatic theocratic groups or simply groups that forcefully opposed the operations and who used terrorist or other asymmetrical methods to obstruct the operations as well as all those who conducted them. Therefore, peacebuilding tools and mechanisms had to be combined with counterinsurgency, which certainly requires responsiveness against asymmetric shocks and terrorist actions, whilst at the same time maintaining the legitimacy of the operations in the conscience of local communities who have not always been supportive of the international actor. Such an experience of the international community in crisis management of the two post-Cold War decades has made the comprehensive approach a very useful organizing principle to be adopted in order to coordinate actions and tools of a different nature and thus address complicated and complex threats of a conventional and nonconventional nature.

#### **4 From a Comprehensive Approach to the Integrated Approach in Managing Hybrid Threats**

The importance of a comprehensive approach in managing complex emergencies and crises lies in its very nature. As an organizational principle, it involves all tools (procedures, policies and resources) to address a threat throughout its numerous development phases. It seeks interconnectedness and transferable links as well as flexibility between different areas of action such as internal and external security, defence as well as social cohesion and economic development whilst presupposing resilience of coordination and decision-making. Today, the nature of modern threats is multifaceted, interdependent and complex. Addressing these challenges and threats often requires a whole complex of different actions aimed at achieving a common goal.

At the international level, the concept of a comprehensive approach, as mentioned above, refers to the use of different (political) tools and mechanisms by many different actors, organizations, governments, international financial institutions, development banks, NGOs, local actors, civil society and local governments in order to tackle an armed conflict and, above all, the phase of building a lasting peace. The international practice of the first two post-Cold War decades has shown that an integrated approach can build and restore the unity of purpose ‘vertically’, i.e. at all levels (strategic, operational and tactical) whilst at the same time can ‘horizontally’ orchestrate various related policies, i.e. in different areas (military, judicial/police, political, economic, development, social and communication [29, 33]. Nowadays,



most international organizations advocate the use of this organizational principle in their actions [21]. At national level, the comprehensive ‘whole of government’ approach has already started to be integrated into state’s strategy. A holistic approach in a national context could be understood as the use of the organizing principle, which requires the integration of all sectors and thus the capacities of state governance (agencies-bodies-ministerial services) under the coordination of a decision-making structure, which would orientate and coordinate the spill-over effect triggered by top-down actions and policies, in order to be able to effectively resolve or manage a multidimensional threat or challenge to the interests of the State. The aim is to maximize the capitalization and the effective use of national resources and capabilities (military, economic, social, cultural, scientific, communication), state-of-the-art technology capabilities as well as those of international actors who share a common understanding with the state authorities, in order to respond to a crisis in terms of resilience (*status quo ante*).

However, as Egnell [7] has convincingly showed, a comprehensive approach in current multifaceted operations has to ensure ‘civil-military integration at the strategic level, but separation of actors and responsibilities in the field of operations’ ([7]: 250). He insists that ‘coordination through unity of command and formal hierarchy should be brought in. These are concepts’, as he rightly observes, ‘that make sense in traditional state governance and military affairs, but are unlikely to attract support within the community-based NGO approach’ ([7]: 250). At the strategic level, a single unified command is cardinal, whilst different actors involved at the lower levels should serve a unified purpose under a pre-existent common analysis and planning.

It is for this reason that a number of governments have adopted an integrated approach in managing international multifaceted including hybrid threats, such as the United Kingdom and the United States, taking the form of whole of government approach), or even Canada whilst they have agreed on the support from different states or institutions. More specifically, as Engell argues, in order to serve this condition, the British government sets up ad hoc committed within the inherently interagency oriented Cabinet office, which works directly for the prime minister rather than the ministries’ ([7]: 252). It is also suggested that another option that would have been employed is ‘the establishment of structures that gather the necessary people from all relevant departments to create a cross-government analysis of and policy towards a problem’ ([7]: 252).

Such an approach, indeed, can be better served at the national level rather than at the international level where international organizations promote their own organizational structure, and thus optimization of a unified single command at the strategic level might require constant legitimization procedures. It is for this reason that countering hybrid threats, as Weissmann et al. [39] advocate, can be better countered through ‘a cross sectoral and cross temporal understanding of the interaction between actors, threats, responses and results’, whilst effectiveness has to be measured and evaluated ([39]: 266). One could argue that it is perhaps the key element in sustaining agility and responsiveness to the evolution of hybrid threats

and respective practices, since a process of constant adaption and adjustment has to be performed.

This is because, as Filipec also insists, the centre of gravity in the context of countering a hybrid attack has to be adjusted according to the nature of the threat which in turn informs accordingly the appropriate response and all those other aspects and spaces with which it interacts [10]. For this reason, one could argue that tools to be used and their effects have to constantly be evaluated by acknowledging that military, as well as primarily nonmilitary disturbing capacities, may require nonmilitary responses. In light of the above, national preparedness and agility in building resilience also take up a comprehensive perspective merging the civilian and military aspects of policy responses.

It is for this reason that transatlantic institutions, NATO and the EU, have both incorporated into their strategies the concepts of resilience at times both giving emphasis on their institutional advantages. Yet, the EU prefers the term hybrid threats instead of hybrid warfare in its documents in order to highlight the security rather than its defence perspective of the planned responses ([24]: 383). By the same token, for NATO hybrid deterrence appears more appropriate. Yet, it should fashion, as Paul Cornish suggests, the notion of ‘Integrated Deterrence’ pointing to a horizontal, vertical, functional and temporal integration of NATO instruments in order to avoid a war [2]. In 2015, NATO adopted its Hybrid Warfare strategy, whilst the EU adopted a year later its Joint Framework for Addressing Hybrid Threats. Importantly it remains to be seen whether its integrated approach in managing crises will be also embrace in practice its commitments on paper.

However, it is worth mentioning that both organizations since 2016 have agreed on a number of activities on which they can unite efforts. As Kremidas-Courtney argues, from the ‘74 areas of deeper cooperation, 20 of which relate to counter hybrid threats. In 2017 the European Centre of Excellence for Countering Hybrid Threats was established in Helsinki destined to support respective cooperation of both organizations’. Moreover, in 2018 NATO ‘also adopted the concept of establishing Counter Hybrid Support Teams (CHST) to give ad hoc assistance to allies in the event of a hybrid crisis’([20]: 2). However, given the differing perceptions amongst its members as regards the importance of hybrid warfare, it remains to be seen NATO’s commitment as well as its approach in the forthcoming strategic concept.

At European level, the EU could not be an exception to adopting a comprehensive approach to crisis management. In 2013, the European Commission reaffirmed the EU’s previous effort to operate on the basis of the organizational principle of an integrated approach in its external action by also setting out their common understanding of both the Commission and the then High Representative regarding the need to further strengthen this organizational principle. In their Joint Communication it is argued that: ‘Comprehensiveness refers not only to the joined-up deployment of EU instruments and resources, but also to the shared responsibility of EU-level actors and Member States’[3].

With the announcement of the Global Strategy for the EU’s Foreign and Security Policy in 2016, the EU now integrates the comprehensive approach to EU crisis

management as one of its priorities. In January 2018, in the Council Conclusions on the Integrated Approach, Member States welcomed the efforts so far to integrate the capabilities of Member States as well as EU services, mechanisms and bodies which can be better coordinated through *a permanent structure within the EEAS (European External Action Service)*, which was certainly created as a major bureaucratic innovation at the service of implementing a comprehensive approach against threats facing the EU and its members including hybrid threats. Apparently, the comprehensive approach can be considered as ‘an integrated approach’ so long as a central body, in this case the EEAS or ad hoc coordination structures, undertakes the coordination of all activities, instruments and policies around which a threat or a multidimensional issue is planned to be addressed even with the cooperation of third-party international actors [3].

Although there is a certain level of ‘useful’ creative ambiguity regarding the way the organizational structure of a comprehensive (integrated), EU approach can be linked to EU Member States’ resilience issues and the EU’s work on security and defence, the EU’s comprehensive approach, as a guideline for action underlines the importance of orchestrating its different capabilities under a coordinated decision-making process. This very acknowledgement can be a useful legacy in the evolution of European security and defence. The modern nature of threats and challenges calls on governments to redefine how to respond to crises. It is not necessary that such crises take the character of a conventional armed conflict. The concept of hybrid threats or hostile actions of asymmetric nature has now been incorporated both into the vocabulary of government decision-makers and strategic international organizations, e.g. NATO, EU and in international literature.

According to the European Commission’s report on hybrid threats, hybrid threats or crises can comprise ‘the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives whilst remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes’ [9].

Some of the most important features of hybrid threats and crises are (a) that they are in most cases below the threshold of a conventional conflict and therefore do not justify an immediate military response; (b) instrumentalize political, social, sporting or other phenomena arising with certain humanitarian aspects in order to disrupt the normal day-to-day life of citizens; c) by invoking a misinterpretation of law or even through a disguised hostile act to affect citizens’ daily lives or state decision-making by disrupting the provision of essential services to citizens, e.g. the supply chain or services relating to critical national infrastructure, such as the supply of electricity or access to the Internet.

However, it is worth stressing that countering hybrid threats is a multifaceted, complex and demanding exercise. It requires a holistic approach involving different actors depending on the nature of the threat. It requires the best possible reading of the situation, the identification and assessment of capabilities, planning and

commitment. Countering hybrid threats requires an environment that is prepared and resilient to disruptions that can affect every aspect of governance.

For this reason, a holistic approach as an organizational principle to be adopted in managing a crisis is extremely important. Its proactive nature *creates resilience* through orchestration and production of response policies at all three levels: prevention, crisis response and recovery. Perhaps one of its serious drawbacks is that it presupposes a lengthy and demanding process based on the robust coordination between the different actors, including the citizens of a state. Nowadays, there are states that take for granted the involvement of their citizens in the implementation of their high strategy [27]. If the *culture of the integrated approach* is created, it is easier to apply in complex emergencies [16], which can result from the application of hybrid threats towards a region.

## 5 Conclusion

A country's National Security and Defence Strategy must incorporate tools to respond to all kinds of threats, not only those affecting the country's territorial integrity or sovereignty but also those affecting everyday life and the protection of its citizens. Thus, when the state, including its constituent societies, continental regions, border regions, big cities, island regions, or strategic regions (transit hubs, ports, railways), and critical infrastructure, is subject to disruptive or coercive action, then an integrated approach to counter such hybrid threats is not a luxury but a necessity.

As already highlighted, the comprehensive approach requires the inclusion of civilian and military response tools whilst it also supports actions to address any problem along the whole spectrum of its development, namely, prevention, response and rehabilitation. As the prevention phase is included in the response planning, this means that the comprehensive approach has the advantage of a proactive action. At each stage, multisectoral orientation is necessary. Therefore, involvement in the design of the whole spectrum of governance, (central government, parties, lobby groups, civil society, and citizens), as well as the whole spectrum of decentralized administration, becomes imperative. This is a difficult multivariable equation that is very difficult to solve in the absence of a common understanding between stakeholders. It is only when citizens, the state as a whole and decision-makers become aware of what the state is constantly trying to secure that the integrated approach becomes a way of thinking.

This is one of the key prerequisites for implementing the above approach in democratic societies. The United Kingdom's logic behind its recent integrated strategy describes in the most eloquent fashion the importance of the integrated approach to countering hybrid threats. In order to substantiate the importance of the integrated approach, it is advocated that the strategy, 'is a response to the fact that adversaries and competitors are already acting in a more integrated way – fusing military and civilian technology and increasingly blurring the boundaries between

war and peace, prosperity and security, trade and development, and domestic and foreign policy. It also recognizes the fact that the distinction between economic and national security is increasingly redundant'. [15].

Therefore, when states are currently called upon to stem but also quickly recover from not only conventional military threats but also from the instrumentalization of actions and practices aimed at disrupting the daily lives of citizens by creating uncertainty in order to block or paralyse the decision-making process, then the response is not limited to defence and security but also to maintaining law and order. As the European Commission states in a formal document, 'Insofar as countering hybrid threats relates to national security and defence and the maintenance of law and order, the primary responsibility lies with Member States, as most national vulnerabilities are country-specific' [9]. Accordingly, each state should in principle operate in terms of self-help and the creation of a national unity of purpose before it invokes or structure more cooperative international response schemes with third parties and organizations.

## References

1. Brinkerhoff, D.: *Governance in Post-Conflict Societies. Rebuilding fragile states.* Routledge, New York (2007)
2. Cornish, P.: *Integrated Deterrence: NATO's 'First Reset' Strategy.* Globsec, Policy Institute, Supporting Paper (2017). [https://www.globsec.org/wp-content/uploads/2017/09/gnai\\_-\\_integrated\\_deterrence.pdf](https://www.globsec.org/wp-content/uploads/2017/09/gnai_-_integrated_deterrence.pdf)
3. Council of the European Union: 5413/18, Council Conclusions on the Integrated Approach to External Conflicts and Crises, 22 January 2018. <https://data.consilium.europa.eu/doc/document/ST-5413-2018-INIT/en/pdf> (2018)
4. Daniel, J., Wittichová, M.: Forging civil-military cooperation: domestic and international laboratories of CIMIC knowledge and practice. *J. Interv. Statebuild.* **14**(5), 596–614 (2020)
5. Dobbins, J.: Towards a more professional approach to nation building. *Int. Peacekeep.* **15**(1), 67–83 (2008)
6. Eaton, J.C., Wing Commander Raf: The beauty of asymmetry: an examination of the context and practice of asymmetric and unconventional warfare from a western/centrist perspective. *Def. Stud.* **2**(1), 51–82 (2002)
7. Egnell, R.: Civil-military coordination for operational effectiveness: towards a measured approach. *Small Wars Insur.* **24**(2), 237–256 (2013)
8. Ehrhart, H.-G.: Postmodern warfare and the blurred boundaries between war and peace. *Def. Secur. Anal.* **33**(3), 263–275 (2017)
9. European Commission: Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats: a European Union response, JOIN(2016) 18 final, Brussels, 6.4.2016. <https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:52016JC0018&from=EN> (2016)
10. Filipec, O.: Preventing hybrid threats: from identification to an effective response. *Eur. Stud.* **8**(1), 17–38 (2021)
11. Franke, V.: The peacebuilding dilemma: civil-military cooperation in stability operations. *Int. J. Peace Stud.* **11**(2), 5–25 (2006)
12. Franke, V., Warnecke, A.: Building peace: an inventory of UN peace missions since the end of the cold war. *Int. Peacekeep.* **16**(3), 407–436 (2009)

13. Fridman, O.: Hybrid Warfare or Gibrinayna Yoyna? *RUSI J.* **162**(1), 42–49 (2017)
14. Friis, K.: Peacekeeping and counter-insurgency – Two of a Kind? *Int. Peacekeep.* **17**(1), 49–66 (2010)
15. Global Britain in a Competitive Age: The integrated Review of Security, Defence, Development and Foreign Policy, 2021, Cabinet Office, <https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy>
16. Goodhand, J., Hulme, D.: From wars to complex political emergencies: understanding conflict and peace-building in the new world order. *Third World Q.* **20**(1), 13–26 (1999)
17. Hickman, K., Weissmann, M., Nilsson, N., Bachman, S.-D., Gunneriusson, H., Thunholm, P.: Hybrid threats and asymmetric Warfare: what to do? In: Conference Proceeding. Swedish Defence University, Stockholm (2018). <http://www.diva-portal.org/smash/get/diva2:1186265/FULLTEXT01.pdf>
18. Hoffman, F.: Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies (2007). [https://www.potomac institute.org/images/stories/publications/potomac\\_hybridwar\\_0108.pdf](https://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf)
19. Kastner, J., Wohlforth, W.: A Measure Short of War. The Return of Great-Power Subversion, Foreign Affairs, July/August 2021. <https://www.foreignaffairs.com/articles/world/2021-06-22/measure-short-war> (2021)
20. Kremidas-Courtney, C.: Building a Comprehensive Approach to Countering Hybrid Threats in the Black Sea and the Mediterranean Regions, NMIOTC, Suda Bay, Crete. <https://nmiotc.nato.int/wp-content/uploads/2020/02/Building-a-Comprehensive-Approach-to-Countering-Hybrid-Threats-in-the-Black-Sea-and-Mediterranean-Regions-by-Chris-Kremidas-Courtney.pdf> (2020)
21. Lasconjarias, G., Larsen, J.: NATO's Response to Hybrid Threats, NATO Defence College. [https://www.files.ethz.ch/isn/195405/fp\\_24.pdf](https://www.files.ethz.ch/isn/195405/fp_24.pdf) (2015)
22. Lindsay, J., Gartzke, E.: Politics by many other means: the comparative strategic advantages of operational domains. *J. Strateg. Stud.* **2020**, 743 (2020). [https://cpass.ucsd.edu/\\_modules/LindsayGartzke2020\\_OperationalDomains.pdf](https://cpass.ucsd.edu/_modules/LindsayGartzke2020_OperationalDomains.pdf)
23. Magnuson, S., Keay, M., Metcalf, K.: Countering hybrid warfare: Mapping social contracts to reinforce societal resiliency in Estonia and beyond. *Texas Nat. Secur. Rev.* **5**, **2022**(2), 28–52. <https://tsr.org/2022/01/countering-hybrid-warfare-mapping-social-contracts-to-reinforce-societal-resiliency-in-estonia-and-beyond/>
24. Malksoo, M.: Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. *Eur. Secur.* **27**(3), 374–392 (2018)
25. Muehlmann, T.: EU civil-military cooperation and the fight against organized crime: lessons to be learned for the Bosnian example. *Eur. Secur.* **17**(2–3), 387–413 (2008)
26. NATO Riga Summit Declaration: para.10, see [https://www.nato.int/cps/en/natohq/official\\_texts\\_37920.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en) (2006)
27. Plummer, M.: When it Comes to Strategy, People are Everything. *The War on the Rocks*, 24 March 2021. <https://warontherocks.com/2021/03/when-it-comes-to-strategy-people-are-everything/> (2021)
28. Ruiz Palmer, D.A.: Back to the future? Russia's hybrid Warfare, revolutions in military affairs and cold war comparisons. In: Lasconjarias, G., Larsen, J.A. (eds.) *NATO's Response to Hybrid Threats*, pp. 49–72. NATO Defence College, Rome (2015). [https://www.files.ethz.ch/isn/195405/fp\\_24.pdf](https://www.files.ethz.ch/isn/195405/fp_24.pdf)
29. Running, S.: *NATO in Afghanistan: the Liberal Disconnect*. Stanford University Press, Stanford (2012)
30. Sari, A.: Legal resilience in an era of gray zone conflicts and hybrid threats. *Camb. Rev. Int. Aff.* **33**(6), 846–867 (2020)
31. Schroeffer, J., Kaufman, S.: Hybrid actors, tactical variety: rethinking asymmetric and hybrid war. *Stud. Conflict Terror.* **37**(10), 862–880 (2014)

32. Siman, B.: Hybrid Warfare Is Not Synonymous with Cyber: The Threat of Influence Operations, Egmont Institute, Security Policy Brief, No. 155, February 2022. [https://www.egmontinstitute.be/content/uploads/2022/02/spb155-siman-final-version\\_0222.pdf?type=pdf](https://www.egmontinstitute.be/content/uploads/2022/02/spb155-siman-final-version_0222.pdf?type=pdf) (2022)
33. Sperling, J., Webber, M.: NATO from Kosovo to Kabul. *Int. Aff.* **85**(3), 491–511 (2009)
34. Strategic Comments: Countering hybrid threats: challenges for the West. *Strateg. Comments.* **20**(4) (2014). International Institute for Security Studies, pp. x–xii
35. Troeder, E.: A Whole-of-Government Approach to Gray Zone Warfare. Strategic Studies Institute, U.S Army War College Press (2019). <https://press.Armywarcollege.edu/cgi/viewcontent.cgi?article=1935&context=monographs>
36. UN Peacekeeping Operations: Principles and Guidelines. [https://www.un.org/ruleoflaw/files/Capstone\\_Doctrine\\_ENG.pdf](https://www.un.org/ruleoflaw/files/Capstone_Doctrine_ENG.pdf) (2008)
37. Van der Lijn, J.: Comprehensive approaches, diverse coherences: the different levels of policy coherence in the Dutch 3D approach to Afghanistan. *Small Wars Insur.* **26**(1), 72–89 (2015)
38. Veljovski, G., Taneski, N., Dojchinovski, M.: The danger of “Hybrid warfare a sophisticated adversary: the Russian “hybridity” in the Ukrainian conflict”. *Def. Secur. Anal.* **33**(4), 292–307 (2017)
39. Weissmann, M., Nilsson, N., Palmertz, B.: Moving out of the blizzard: towards a comprehensive approach to hybrid threats and hybrid warfare. In: Weissmann, M., Nilsson, N., Palmertz, B., Thunholm, P. (eds.) *Hybrid Warfare. Security and Assymetric Conflict in International Relations*, pp. 263–272. I.B. Tauris (2021)
40. Wirtz, J.: Life in the “Gray Zone”: observations for contemporary strategists. *Def. Secur. Anal.* **33**(2), 106–114 (2017)
41. Zanoti, L.: UN integrated peacekeeping operations and NGOs: reflections on governmental rationalities and contestation in the age of risk. *Int. Peacekeep.* **17**(1), 17–31 (2010)

# European Union and NATO Cooperation in Hybrid Threats



Mikhail Kostarakos

This Chapter captures the perception of two important international organizations on the newest form of warfare: Hybrid. In order to clarify not only the term but also the perception on it, we need to take things from the beginning.

The term “hybrid force” was used for the first time in 1998 by US Navy (USN) Lieutenant Robert G. Walker in his thesis at the US Naval Postgraduate School, on “*US Marine Corps (USMC) Special Operations.*” The term was attributed to the USMC that historically has demonstrated itself as a “*hybrid force,*” capable of conducting operations within both the conventional and unconventional realms of warfare. This tradition was continued to the present day with the Special Operations capable Marine Expeditionary Unit (MEU) (a joint amphibious brigade size formation) described as “a Hybrid force for Hybrid Wars” [1]. The term “*Hybrid,*” of Latin and Greek origin, is used to indicate an organism, or a product or an offspring of mixed character; composed of different elements, or different parents.

The first question on the hybrid term pops up immediately: Why this terminology was suddenly adopted at the beginning of twenty-first century as the terminology of choice, by not only NATO and the EU, but also by Russia and other global powers?

As the Prussian theorist of war, Carl von Clausewitz, argued, war is an ever-evolving, interactive phenomena. Understanding the complexity and distinctions of various modes of warfare conducted across the continuum of conflict is critical, as is understanding our adversaries, their methods, and conceptions of victory. To better understand this, let me guide you in a small historical journey [2].

---

General Mikhail Kostarakos (Ret.)  
Former Chief of the Hellenic National Defence General Staff  
Former Chairman of the European Union Military Committee  
(General Mikhail Kostarakos passed away before the publication of this work was completed.)

---

M. Kostarakos (✉)  
Hellenic National Defence General Staff, Athens, Greece



The US Marines and their scholars were not the ones who invented neither the term nor the necessity for this warfare combination. War, in the form of an armed conflict, is indigenous in human history since man first appeared on earth. Ancient Greek, Chinese, and Roman history is full of paradigms of combined use of military brutal force, together with nonlethal, religious, diplomatic, economic or any other nonmilitary means based on assessments tailored to the adversaries.

In the Middle Ages and in Renaissance, although brutal military force was used extensively, it is now very well known that the Byzantines, as well as some Italian city-states, were using the military force as their last resort. Their preferred *modus operandi* included active and extensive engagement of spies, ambassadors, bribers, monks, priests, and the offer of ransoms, all kinds of gifts, beautiful princesses offered as wives, as well as “exclusive intelligence” that God is standing by them and against their adversaries. It was still warfare, but the pikes, the muskets, the swords, and the cannons were absent or carefully hidden under heavy, rich, and impressive clothing and piles of coins or gold and gifts.

Gradually, the ancient Phalanx and the Roman Legions were replaced by Regiments of Blue, Red or Green coats in close line, conquering or defending territory in human squares against saber-rattling cavalry charges and artillery explosions. Big men, big horses, big rifles, big sabers, big moustaches, huge formations, genius military thinking, lots of strength, lots of courage, lots of bravery, and eventually, lots of blood.

The two World Wars of twentieth century with the tenths of millions of casualties, and the estimated total destruction and hundreds of millions of deaths in case of a possible thermonuclear war during the Cold war that followed suite, reminded to the decision-makers and to the politico-military scholars that another way should be found in order to impose our own will to the adversaries.

In the meantime, the Soviet Union understood that they had at their disposal a spiritual weapon of equal power with religion: the ideology of communism. And they started using it, exactly the same way various religions were used by various actors in the previous centuries.

In a lot of cases and in a lot of countries (not everywhere though), there was no need for columns of battle tanks to invade or to occupy a country. Ideology, political maneuverers, exploitation of personal vulnerabilities, subversion, guerilla groups and tactics, unconventional warfare, press influence and fake news, undermining, corruption, and blackmailing became the new weapons of choice in this different type of warfare. Sometimes the traditional military means were used in conflicts but most of the time this was due to necessities and impossible to avoid confrontations and certainly not as the first choice. This period known as Cold War, saw little combat action and little blood by the Great Powers, but a lot of bloody proxy wars, as well as intense political, diplomatic, economic, and ideological activities and skirmishes that could achieve the same results as the bloody wars of the past.

When the Soviet system collapsed, new ideologies started filling the gap: globalization and liberal order together with Islamism. A new charter for the combined forms of Warfight started and this time it was called “Hybrid.” This term was immediately adopted by everyone. Most of the academia, ignoring the first

appearance of the term in 1998, they gave credits for the term “*Hybrid Warfare*” to Major USMC William J. Nemeth at his thesis, again at the US Naval Postgraduate School, on “*Future War and Chechnya: A Case for Hybrid Warfare,*” in 2002 [3].

Another USMC military theorist, LtCol (retired) Frank Hoffman significantly contributed to the popularization of the term, studying hybrid through historical examples of deliberate creation of uncertainty within the battlespace, challenging thus the conventional military thinking. It was him, like a modern apostle of Hybrid Warfare who used this term to describe Hezbollah tactics and strategies as seen in the summer 2006 battle between Israel and Hezbollah in Lebanon. Hezbollah clearly demonstrated the ability of nonstate actors to study and deconstruct the weak points and vulnerabilities of Western style militaries, even of one of the best among them like the Israeli Armed Forces, and to devise appropriate counter measures with surprising effective results [4]. The term gained immense popularity and further proliferated and mainstreamed from 2008 onwards, largely due to its adoption by NATO’s Allied Command Transformation (ACT) and the interconnected nature of military and policy makers within NATO.

In the US, the officials in their effort to sustain the world dominance jumped on the wave. In their Strategies and Defense Reviews starting from 2006, they quite properly recognized that future challenges will avoid the US overwhelming military strength and seek alternative paths. New investments were required for this nonmilitary nature of challenge and the Pentagon was obliged to set its mission and capabilities beyond its preference for fighting conventional forces in battles against preferred enemies and be ready now to fight against irregular but thinking opponents, instead.

This rise of the Hybrid Warfare concept however, does not represent the end of traditional or conventional warfare. The bloody terrible warfighting remains always “alive”; this new term just inserted a new complicating factor for defense planning in the twenty-first century. It also made clear to politico-military planners that future opponents in this realm will be dedicated, will learn rapidly, will adapt quickly to more efficient modes of killing already tested at the Twin Towers attack, and they will not remain focused on low-tech applications.

The benchmark of the new era of war was already there. The tragic attack of September 11, 2001 clearly punctuates the end of the war as we knew it and awaken everyone to the dawning of the new one. None is entitled to be surprised, if they had studied military history in the past. It is well known that Clausewitz has recognized that every age has its own conception of war and although globalization has made war more dangerous, the emergence of Hybrid Warfare in our time is one more undeniable justification of Clausewitz’s theory.

In effect, Hybrid Wars blend the lethality of state conflict with the fanaticism, the ruthlessness, and the protracted fervor of irregular warfare. The term “Hybrid” captures both organization and means [4]. Hierarchically, political structures will always remain at the top, but this will be coupled with a decentralized networking of semi-independent cells, representing the tactical level and a loose or practically nonexistent command and control system. Cunning savagery, continuous

improvization, and rampant organizational adaptation combined with a polymorphic nature, will finally mark this new form of warfare.

As always in the planning process, the starting point is the identification, understanding and proper assessment of the threats and challenges in the hybrid domain and how they differ from the more conventional “nonhybrid” ones. For a threat to be of Hybrid nature, it should be the product and the mix of different origin and methods, conventional and nonconventional, military and nonmilitary, new and old, modern and traditional. In this sense, not all threats appearing today are of Hybrid nature or have Hybrid characteristics. And this needs to be clearly understood by all planners. On the other hand, terrorism, trafficking of all kinds, cybercrime, criminal activity, and extortion are not Hybrid per se in nature. They may become Hybrid, depending on how and to what extent they will be used, by whom they will be pursued simultaneously, and by using what kind of multiple tactics.

It seems that there are no limits at the Hybrid landscape. There is a possibility that threats emanating from a particular organization or state are Hybrid while others coming from the same actor are not. A continuously reviewed threats assessment, in light of new developments or policies, is paramount for the situation awareness.

We conclude that in general terms, Hybrid Threats are characterized by:

- A capacity to identify and the ability to exploit the vulnerabilities and the weak points of the targets across the political, military, economic, social, informational, and infrastructure (PMESII) spectrum, in ways that were not previously considered
- A combination of conventional and unconventional, military and nonmilitary, overt and covert actions
- A wider set of military, political, economic, and civil information (MPECI) tools and techniques that cannot usually be found at traditional threat assessments
- An effort of creating confusion and ambiguity on the origin, the nature, and the aim of the threat
- A difficulty to be identified as Hybrid until it is well underway, with damaging effects having already begun manifesting themselves and degrading a target’s capability to defend itself
- A synchronization of means in novel ways
- A capacity of keeping the level of hostility below any threshold of conventional war or armed aggression and therefore to stay out of any UN Charter and International Laws and Conventions on War and Conflicts provisions and jurisdiction [5]

On the other hand, Hybrid Threats are not:

- Defined by their actors or origin, since states, nonstate actors, and even individuals might be considered as such
- Related to some specific technology, because this list keeps growing, as new technologies become available

- Aiming to specific effects, as a hybrid campaign may result in different outcomes, such as human casualties, decision changing, government swap, social or economic destruction, altered public perception, etc. [5]

All in all, perhaps the best way to put it, is that “Hybrid Threat” could be a clear manifestation of a Total War (an “*Anything War*”) but out of any classical definition of conflict or war, and below all armed aggression or conflict thresholds.

Based on all these considerations, we may proceed to an initial definition of “*the Hybrid Opponent*” profile:

*“The Hybrid Opponent, seeking to exploit the full range of target’s weaknesses, possesses the capacity and the initiative of simultaneous escalation at different points along a broadly defined spectrum of conflict, moving beyond the limits of any battlefield at will, in order to target state or society. At the same time, he may use different channels and proxies for unlawful actions, often making not only attribution difficult but also identification of clear strategic objectives almost impossible” [5].*

There are many types of state and nonstate actors which potentially could be our “*Hybrid opponents*” and may create Hybrid Threats by leveraging at least two of the following key entities:

- Military force
- Nation-state owned paramilitary force (internal security forces)
- Insurgent groups
- Guerilla units (irregular forces operating in territory)
- Mercenaries
- Foreign Intelligence Services
- Transnational or subnational political movements
- Criminal organizations (gangs, drug cartels, hackers)
- Transnational corporations
- News media
- Idealists’ groups
- Activists’ groups
- Amateur hobbyists
- Religious movements
- Various Foreign Fighters
- Isolated idealists/“warriors”/activists known as “*Lonely Wolfs*” [5]

These actors may cooperate by pursuing common objectives, thus allowing them being adaptive and difficult to define.

Hybrid threats can also be created by a state actor using a proxy force. A proxy force sponsored by a major power can generate hybrid threats readily using advanced military capabilities provided by the sponsor. Proxy wars, appealing to some as “*warfare on the cheap*” are historically ubiquitous but chronically understudied. The hybrid threat concept captures the ongoing implications of globalization, the diffusion of military-related technologies, and the information revolution. Hybrid threats are qualitatively different from less complex irregular or militia forces. They, by and large, cannot be defeated simply by Western

counterterrorism tactics or protracted counterinsurgency techniques. Hybrid threats are more lethal than irregular forces conducting simple ambushes using crude improvised explosive devices, but they are not unfamiliar to Western forces and can be defeated with sufficient combat power [2].

Now that we have described Hybrid Threats, challenges, and opponents, we may finally turn the famous and universally accepted Frank Hoffman's definition of Hybrid Wars which largely contributed to establishing hybrid in US and eventually NATO military thinking:

*"Hybrid Wars can be conducted by both states and a variety of nonstate actors. They incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. These multimodal activities can be conducted by separate units, or even by the same unit but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects. The effects can be gained at all levels of war" [4].*

Continuing in the historical and definition's part, a new question emerges: To whom these labels of Hybrid Threats and Opponents are ascribed, within the contemporary geopolitical framework? If Hybrid Warfare characteristics, as some scholars argue, were deduced from "*looking at the enemy*," then who the enemy is and what should we do about it?

In Western perceptions, Russia is the embodiment of an actor conducting Hybrid Warfare. Events in Georgia, Crimea, and Eastern Ukraine have led US, NATO, and EU security officials to pay greater attention to Russia's assertive behavior and its ways of war. Russia's Soviet past pays its toll as well. For these reasons, Hybrid Warfare is now an explicit discussion point among NATO and EU military and civilian leaders.

Numerous intelligence sources describe President Putin's preferred method as "Hybrid Warfare," identified by him as a blend of hard and soft power. Indeed, according to a statement by Putin in 2006, Russia's approaches to conflict "*are to be based on intellectual superiority. They will be asymmetrical, and less costly.*" He then told the Defense Ministry Collegium in 2013 that the Armed Forces must reach a "*new level*" of capability within 5 years due to the "*dynamics of the geopolitical situation*," again emphasizing the need to develop capabilities. A rich Hybrid toolbox containing military and nonmilitary tools, diplomatic, social and economic, their use choreographed by surprise, and facilitated by ambiguity in both source and intent, will eventually confuse and wear down most of the opponents, making it hard for multinational bodies such as NATO and the EU to craft a response.

According to western intelligence experts, the Russians have been able to combine various military forms of warfare with economic, information, and diplomatic means into a Hybrid Threat based on "Whole of Government Approach" maximizing advantages for Russia, as well as minimizing risks and cost. This approach adds a new dimension to Hybrid Warfare. It is not only that Hybrid Warfare is deduced from "*looking at the enemy*, but it was also deduced by *looking in the mirror*." This means that Hybrid Threats could be the product of a sudden NATO and EU realization of their own weakness and vulnerabilities

when faced with an increasingly uncertain environment in which Russia has the initiative. Russia's adoption of Hybrid Warfare then is normal, being the product of a combination of strategic opportunity and necessity, tailored to today's global environment, characterized by heightened societal connectivity, fragility, and vulnerability. Kremlin is pursuing objectives of the highest importance through the active, but calibrated employment of mostly nonmilitary means together with the necessity to avoid a highly destructive and decisive use of force by an adversary [6].

For some Western experts, it is now clear that the West must adjust to the situation in which it now finds itself in relation to Russia to a "*permanent Hybrid War*" referring to Russian General Gerasimov statements and his famous "Gerasimov Doctrine." Although the existence of this Doctrine was put into question, whether it was an official Doctrine by the top Russian military officer (Chief of the General Staff) or just some impressive headlines of an explicit interview, being able to evaluate Russian intent on this subject, it is and will remain paramount for the West. According to the "Gerasimov Doctrine": "*...In the twenty-first century, Russia has witnessed a tendency toward blurring the lines between war and peace and in recent conflicts, methods of conducting military operations that cannot be considered purely military have emerged. The role of nonmilitary means in achieving political and strategic goals had grown, and in many cases exceeded the power of force of weapons in their effectiveness. All this, is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces. The open use of forces—often under the guise of peacekeeping and crisis regulations—is resorted to only at a certain stage, for the achievement of final success in the conflict. This is often coupled with asymmetrical actions that have come into widespread use, and are enabling the nullification of an enemy's advantage in armed conflict through the cross-over of different domains.... Long-distance, contactless actions against an enemy through the use of cyber elements are being combined with the use of special operations forces, internal opposition and informational action, devices and means that are constantly being perfected, in order to achieve combat and operational goals.... In conclusion, no matter what forces the enemy has, no matter how well-developed his forces of armed conflict may be, forms and methods for overcoming them can be found. The enemy will always have vulnerabilities and that means that adequate means of opposing him exist*" [7].

Maybe what was perceived as the "Gerasimov Doctrine" was nothing more than his understanding of the current character of the warfare. There is no doubt that the Russian understanding of conflict constitutes a full spectrum approach which means it can include measures short of war or more violent Hybrid approaches as appropriate to the situation. Historically, Russia's approach has appreciated the value of indirect approaches and nonmilitary instruments, without however disregarding or neglecting Hard power. The West would do well to better relearn Russia's strategic culture and history and especially the part inherited from the Soviet Union.

In reality, after the first attempt at the Israel Hezbollah conflict in Lebanon, Russia with its invasion and annexation of Crimea and the following operations

in Ukraine offered to the Hybrid Warfare the first crash and reality check. The theoretical assumptions and hypotheses of Western scholars appeared suddenly at the 8 o'clock TV News and started keeping worried and busy western political and military decision-makers and scholars.

But this is not exclusively a European or Atlantic issue. China remains a very old player who recently reemerged at the global scene. One should not forget that the Sun Tzu writings about winning wars without giving battles were the real incentive and leverage of this form of warfare. As Western scholars discovered, China is well organized to conduct operations short of military conflict. Chinese employ diplomatic pressure, rumor, false narratives, and harassment to express displeasure, assert hegemony, and convey threats. Guided by their doctrinal principle of "dis-integrating enemies," conducting "political warfare," they promote the suppression of perceived threats with the use of Psychological Operations in order to influence policies of friends and foes as well as propaganda amplifying or attenuating the political effects of the military instrument of their national power. At the same time, Chinese hybrid operations conducted against and inside neighboring countries suggest that Beijing's doctrine is much more than merely academic [2].

Analysts from Chinese People's Liberation Army (PLA) contributed to the Hybrid theory as well. They argue that future wars will be marked by the "three Non" warfare(s):

- Noncontact
- Nonlinear
- Nonsymmetric

In "Noncontact warfare," which sounds more and more as their preferable course of action, the more technologically advanced adversary exploits its advantage by staying outside the reach of opponent's weapons while retaining its ability to directly target and strike its rival. China's conception of "Quasi-War," (a term referring to an undeclared, although fiercely conducted, mostly naval form of warfare) which is part of their Conception of Military Operations (Wartime-Quasi War-Nonwartime) widely known as "Three War Concept," clearly embraces "legal, psychological, and information (media) activities" short of war, while at the same time builds up national power, increases conventional military capabilities, and extends its military reach. It remains to be seen to what extent China will retain an interest in Hybrid Warfare when it will obtain global parity or superiority. Moreover, a convergence of Russian and Chinese Hybrid tactics has been observed taking place recently, emanating from Chinese interpretations of Russia's actions in the Crimea and the Cyber Cloud, while at the same time a possible Chinese success in the East China Sea or Taiwan issues may be copied by Russia in its international relations [2].

Russia however, is not the only perceived Hybrid Threat by the West. In the current European security environment, the other major Hybrid Threat is perceived to be the Al Qaida Islamic Organization, the Islamic State (IS) known also as ISIS or DAESH, and various sister-organizations of Islamic extremism and/or terrorism in the Middle East or Africa. ISIS has shown a high level of expertise, knowledge,

and professionalism on hybrid issues, exploiting effectively and successfully all hybrid tools it had at its disposal. They created, managed, and spread out terror in such a way that made the multibillion New Iraqi Army to collapse without big battles within weeks. It took a global “Coalition against Terror” under US leadership to fight against it and finally defeat it with the use of excessive military power. France was the first in this approach having in mind the jihadist nexus in Sahel and together with NATO Parliamentary Assembly, they both classified Islamic State as Hybrid Threat [6]. This was due to its effective ability to employ a range of tactics from terrorism to conventional, and its global recruiting and operational networks, combined with effective use of media in order to generate fear and intimidation and to accelerate even “lonely wolf” recruitments. It is obvious that all these are perfectly fitting to the characteristics of the Hybrid Threat [8].

In addition, the instrumentalization of migration can be used as a tool for hybrid war. In this context, the military power projection and the aggressive policy, along with the constant violations of national sovereignty (Hybrid tools by definition), have been combined in the past from different actors with the uncontrolled sending of refugees and immigrants to violate borders. This is a Hybrid invasion that is designed to create problems in other countries, forcing them to succumb to geopolitical and economic demands. Above all, this Hybrid invasion is expected to create a huge social, economic, and security problem in these countries. The Hybrid nature of this migratory “invasion” is therefore self-evident, and should be considered as Hybrid because it is carried out by unarmed civilians.

With this Hybrid Operation, the actor seeks to implement the usual *modus operandi* which always leaves the adversaries with only two choices: whether to agree with the actions, demands, and “*faits accomplis*,” or to face massive and uncontrollable Migration, with the opening of the borders and the massive and uncontrolled exodus of poor immigrants and refugees, or in another Hybrid variation, to face sometime in the future in the context of an immediately exploitable crisis, actor’s huge and strong army. The aim is, through the use of Hybrid tools and without any conventional warfight, to revise the existing geopolitical situation and the borders and to gain serious political and financial benefits from the target countries.

An effort to identify what the West and its two main international organizations are doing to protect their status and their citizens from all those “Hybrid Threats,” is necessary.

At the beginning, Hybrid Warfare became the buzzword of choice for NATO and later for the EU. Unsurprisingly, there was no common understanding of the term among NATO Allies and EU Member States.

NATO was the first to develop an approach toward Hybrid Warfare. Differentiated perceptions of Hybrid were surfaced by NATO experts, against the established term which should be seen as just another form of warfare in the twenty-first century, where an adversary can use every means in its power and Hybrid should not definitely be put on a pedestal. In addition, Hybrid Warfare was an opportunity for the military defense planners to remain relevant, to remain involved in NATO defense planning and in crisis response measures, and to guarantee for the military a



sustained level of attention. In the meantime, the officials acknowledged that NATO was seeing Hybrid as *“a form of warfare aiming to destabilize and make a country more attackable,”* providing at the same time *“a useful, holistic understanding of the security challenges from both the East and the South”* and tools for a comparative strategic perspective while allowing for a differentiated response.

Nevertheless, NATO’s approach to hybrid seems largely connected to a previously “dominating term,” known as “Comprehensive Approach,” a by-product of Alliance’s experiences in the Balkans and Afghanistan. During these crises, NATO recognized that the military cannot resolve crises or conflicts by itself. Achieving acceptable and sustainable solutions requires capabilities that the military alone cannot provide. A comprehensive political, civilian, and military approach is necessary to effectively manage today’s complex crises. NATO’s Comprehensive Approach therefore, can be understood as a concept, philosophy or mind-set rather than a documented process or capability. It is also better to speak of “a” Comprehensive Approach instead of “the” Comprehensive Approach. Moreover, NATO decided to not develop and publish any definition on what Comprehensive Approach exactly is, not to claim ownership. Even NATO Secretary General, Stoltenberg, in his effort to achieve continuity to NATO’s Adaptation efforts stated that *“hybrid is the dark reflection of our Comprehensive Approach”* and started talking about *“preparing for, deterring, and defending against”* Hybrid Warfare [6].

Following the three “Ds” rule, although with Dialogue or Collective Defense there were clear guidance and plans, with Deterrence the situation was more complicated. Hybrid was assessed as less deterrable and deterring Hybrid as such, not really useful for the Alliance. To this end, the new idea of “Deterrence by denial” was established within the Alliance. This concept is based on reducing the perceived benefit of an action by hardening the defense and making unbearable for the opponent the cost of a potential attack. This form of “Deterrence by denial,” although initially counterproductive and costly, is expected to bring better results than the low-success possibilities of “Deterrence by punishment,” another form of deterrence which aims to persuade the adversary that the cost of achieving its objective will be prohibitive. All these second thoughts make finally another form of deterrence, “Deterrence by resilience” the new, logical, and natural choice for Hybrid Warfare NATO’s defense planning [6].

Cyberattacks, one of the main tools in the Hybrid toolbox, made the Allies realize the importance of resilience. Ensuring the survivability of governments and the endurance of state mechanisms, resilience of critical infrastructure, services, and societies, is a very important tasking, because it complements NATO’s Military Mobility. This is a common NATO-EU project guaranteeing fast mobility and deployment of Allied troops throughout Allied territory in order to counter Hybrid Warfare. In addition, NATO developed guidelines to enhance national resilience and established a new civil-military Intelligence Division in NATO HQ in Brussels, in order to persuade Allies to share intelligence, something that is a paramount factor for the identification, understanding, knowledge, and anticipation of Hybrid Threats [9].

Moreover, Hybrid Threats are qualitatively different from threats emanating from less complex irregular or militia forces. Since it is important to distinguish between Hybrid and Irregular Warfare, a revised definition of Hybrid related to Irregular Warfare could be:

*“The purposed and tailored violent application of advanced conventional military capabilities with irregular tactics, with terrorism and criminal activities, or combination of regular and irregular forces, operating as part of a common design in the same battlespace.”* The addition of the word “violent” to a Hybrid definition is particularly telling [2].

As NATO Secretary General, Stoltenberg recently stated describing the NATO reaction to the ongoing Hybrid Threat situation, *“Hybrid methods of warfare, such as propaganda, deception, sabotage, and other nonmilitary tactics have long been used to destabilize adversaries. What is new about attacks seen in recent years is their speed, scale, and intensity, facilitated by rapid technological change and global interconnectivity. NATO has a strategy on its role in countering hybrid warfare and stands ready to defend the Alliance and all Allies against any threat, whether conventional or hybrid.”* The main points of this strategy are the following:

- The primary responsibility to respond to Hybrid Threats or attacks rests with the targeted Nation.
- NATO is prepared to assist any Ally against hybrid threats as part of Collective Defense. The Alliance has developed a strategy on its role in countering Hybrid Warfare in order to help addressing these proper threats.
- In July 2018, NATO leaders agreed to set up Counter-Hybrid support teams, which provide tailored targeted assistance to Allies upon their request, in preparing against and responding to Hybrid activities.
- NATO is strengthening its coordination with partners, including the European Union, in efforts to counter Hybrid threats.
- NATO’s Joint Intelligence and Security Division has a hybrid analysis branch that helps improve situational awareness.
- The Alliance actively counters propaganda—not with more propaganda, but with facts—online, on air, and in print [10].

In sum, NATO’s approach and reaction to Hybrid Threats and Warfare can be described as military-centric, pragmatic, not over-obsessed by the nature of Hybrid Threats, based on and sustaining Comprehensive Approach and finally effectively protecting the Allied Centers of Gravity which are the Allied Solidarity and Cohesion.

At the same time, and in the same geopolitical landscape, another international actor appeared to be particularly better fit for addressing Hybrid, namely the European Union.

In general, the EU keeping distances from whatever has to do with the military, avoided the term “Hybrid Warfare” and preferred the term “Hybrid Threats.” The usual lack of coherence was obvious when the Union, failing to agree to a definition, started crafting a number of policy responses. In a video released by the Council

of the EU, “Hybrid Threats” were described as “*a combination of military and nonmilitary means having the objective to destabilize opponents, create confusion, mask the real situation on the ground, and hamper decision-making.*” To understand the EU’s relaxed approach to Hybrid Threats, one should have in mind that already in 2015, the then EU High Representative and Vice President of the Commission (HR/VP) Mrs. Federica Mogherini called them “*the new normal*” [6]. During the same period, a number of Member-States (MS) started drafting nonpapers on Hybrid, focusing on different issues. So, the Nordic Group’s nonpaper was focusing on Russia, the French one on the Southern flank, and the Finnish on resilience. The Latvian and Luxembourgish EU Presidencies drafted background notes providing context and recommendations on possible ways forward, following a tasking to the Crisis Management Planning Directorate (CMPD) of European External Action Service (EEAS) to draft an initial paper for discussion, circulated in May 2015.

Officially, however, the process started with the invitation of the Foreign Affairs Council to the European Commission (EC) and HR/VP in May 2015, to draft a joint framework on Hybrid Threats “*with actionable proposals.*” The EU, as always, sought taking all MSs’ concerns into consideration. This all-inclusive approach led to confusion within the EU. The inability to provide a clear definition was called “*need for flexibility,*” while the then CMPD Director Amb. Gabor Iklody stated that “*hybrid is just a bumper-sticker*” and that “*there is no need for a definition . . . as long as we know what we mean by it.*” Within the same context, the CMPD stated in an early document that:

*“Hybrid warfare can be more easily characterized than defined, as a centrally designed and controlled use of various covert and overt tactics, enacted by military and/or nonmilitary means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces.”*

Eventually, the CMPD prominence in shaping the EU’s overall response to Hybrid Warfare resulted to an approach similar to NATO. CMPD authors argued that “*Hybrid attacks are designed to exploit country’s vulnerabilities*” and can “*generate ambiguity both in the affected population*” as well as internationally with the “*aim to swamp a government.*” This emphasis on vulnerabilities leads directly to the issue of “*building resilience*” and finally on “*how the EU sees its role in countering them?*” [6]

Although there is no doubt that the EU is better placed than any other organization to counter Hybrid Threats, the EU officially recognized that “*responding to and countering them, is and will remain national responsibility,*” and the Union’s role is described as a platform for harmonizing responses on specific issues, as well as providing added value on awareness, resilience, and response.

This EU’s approach to countering Hybrid Threats materialized in April 2016, when the Council welcomed the “*Joint Communication on countering Hybrid Threat and fostering resilience of the EU and its MS as well as Partners*” [11] and invited the Commission and the HR/VP “*to provide a report by July 2017 to assess progress*” on the topic, highlighting “*the need for closer dialogue, coordination, and cooperation with NATO.*”

In July 2016, following the bold launching of the EU Global Strategy, the leadership of the EU together with the Secretary General of NATO, signed a Joint Declaration in Warsaw with a view to giving new impetus and new substance to the EU-NATO strategic partnership. Two years later, in 2018, the leaderships of EU and NATO signed a second Joint Declaration in Brussels, calling for swift and demonstrable progress in implementation [12].

The Declarations outlined 74 concrete actions in seven areas where cooperation between the two organizations should be enhanced. One of these areas is “Countering Hybrid Threats,” including ten concrete actions. Five progress reports have been submitted highlighting main achievements and added value of EU-NATO cooperation in different areas.

The study of these documents is essential for the understanding of EU’s reaction to Hybrid [13]. To this end, the EU identified three steps besides Cooperation with NATO:

- Awareness
- Resilience
- Response

The first step of the EU reaction to Hybrid Threats involves “improving awareness” and a key element of this is establishing a clear understanding of exactly what Hybrid Threats are and how they differ from non-Hybrid ones. Not all contemporary threats are Hybrid. It is well accepted now that Hybrid Threats are the mix of different methods—conventional and unconventional, military and nonmilitary—and this is what makes a threat Hybrid. This is a clear position to the usual debate when such new concepts appear, whether conceptual clarity is necessary in order to craft a sound policy response or constructive ambiguity is preferable. Eventually in Hybrid Warfare this is not the case. Both the HR/VP and the MS were encouraged to launch their own “Hybrid risk surveys” and the Commission to take actions in order to identify common tools and indicators for the protection of critical infrastructure, as well as to “*promote and facilitate information sharing platforms and networks*” in cyber security. The flagship initiative to address the ambiguity of Hybrid was the creation of an “EU Hybrid Fusion Cell” within the “EU Intelligence and Situation Center” in order to:

- See the patterns of a Hybrid Campaign in intelligence provided by MS and EU Bodies
- Cooperate with NATO
- Provide top EU decision-makers with better situation awareness [14]

Moving to the second and the third steps of EU’s reaction to Hybrid Threats, identify “resilience” and the “response as appropriate.” The multilayered and multifaceted nature of this kind of threats calls for an equally multipronged response, theoretically embracing the widest range of actions, with a view to “building resilience” and “responding to attacks.”

Although the first approach on countering Hybrid Threats has mainly been military-centric, and this is valid especially in the context of NATO, the nonmilitary

and predominately unconventional nature of this kind of threats arguable require their tackling to be done through nonmilitary means and civilian approach. Most importantly, in an EU context, it is the mix and continuity of external and internal security policies and instruments which are likely to provide the most appropriate response.

EU therefore is in need of a specific kind of policy based on the balanced use of Smart Power. It was initially known as EU Comprehensive Approach Policy, not to be confused with NATO's policy with the same name. Later became known as "Integrated Approach Policy to Conflicts and Crises" and became a strategic priority for EU external action. It entails a more coherent use of the various policies and instruments at the disposal of the EU, ranging from conflict prevention and diplomacy, security and defense to development, governance, humanitarian aid, trade, and finance [15]. As these policy domains are under the remit of various EU bodies and institutions, implementing the integrated approach requires a high degree of coordination, while also respecting different mandates, roles, legal frameworks, and chains of command. In operational terms, any EU-wide response Policy would need to feature responsibilities and identify synergies among four sets of actors and/or instruments:

- Member States (MS) instruments and activities
- EU internal security instruments (security, justice, etc.)
- EU external security instruments including CSDP Operations and Missions
- NATO activities on the same issue or area [3]

Exploring the idea of deterrence which should be included in EU responses to Hybrid Threats, the focus here again remains in resilience. Although the EU officially is not mentioning deterrence and unofficially the EU people announce that "*we do not deter*," several elements do point in this direction. Deterrence-like signaling can easily be identified in the possible invocation by any MS of the Article 42.7 of the Treaty of the EU requesting "Mutual Assistance" in case of multiple serious Hybrid Threats constituting armed aggression against this same MS (as happened in 2016 following the terrorist attacks in Paris). This can be easily assessed as "Deterrence by Resilience" or "Deterrence by Mutual Assistance." "Deterrence by Resilience" through increased cooperation with NATO, was observed in the coordinated NATO-EU response at the refugee crisis in the Aegean Sea in 2016, with the objects of resilience being mainly Greece and the EU MS adjacent to the area or at the end of the "refugee corridor" in Austria, Germany or Sweden.

Moreover, although economic sanctions are considered as EU's sole Hard Power tool, the very interesting following sentence can be found in the EU Joint Framework on Hybrid Threats:

*"In the context of CFSP (Common Foreign and Security Policy) instruments, tailored and effective restrictive measures could be explored to counter Hybrid Threats" [14].*

Overall, although the EU indeed, for obvious soul-saving political reasons, does not subscribe to the deterrence concept, this does not mean that EU will not use "Deterrence by Denial" when necessary, by using the proper denial toolbox.

To conclude, the EU's response to Hybrid Threats, can be seen as a mix of existing measures together with new attempts to improve situational awareness and address vulnerabilities. Although the first line of defense will likely (and maybe should) remain with MS, the EU needs to demonstrate its added value when it comes to improving awareness, building resilience, and responding to attacks. The response should include:

- The existing national policies combined with cooperation at EU level at the sectors of law enforcement, border control, antidrug, anti-trafficking, anti-terrorism, and intelligence sharing
- Possible EU initiatives aimed at capacity building in third countries or disrupting hostile activities whenever they take place
- The development of various sectoral strategies (most of them delivered already) like maritime, or cybersecurity, and finally a broader "Global Strategy" as happened in 2016 [16]
- Synchronization of all these aspects, in a tailor-made fashion

While NATO-EU cooperation outside the "Berlin Plus" arrangements and due to, from time-to-time, US controversial position on this issue, is mired by political obstacles, in the context of Hybrid Warfare, a new dynamic of engagement has emerged [6]. Due to a perceived urgency, MS and Allies granted more space to the staff members of both organizations to improve cooperation, find synergies, and progressively deepen their relationship. Despite the slow progress and the ups and downs of formal EU-NATO cooperation, Hybrid set the tone for closer NATO-EU Institutional relations, paving the way for subsequent developments in EU-NATO cooperation. As it was stated in a Joint Communication to the EU Parliament "*The High Representative, in coordination with the Commission, will continue informal dialogue and enhance cooperation and coordination with NATO on situational awareness, strategic communications, cybersecurity and 'crisis prevention and response' to counter Hybrid Threats, respecting the principles of inclusiveness and autonomy of each organization's decision-making process*" [14].

In general, the discussion on Hybrid Threats significantly contributed to further NATO-EU coordination. Indeed, while both the EU and NATO see their MS and the Allies as the first responders in Hybrid crises, it became clear that closer cooperation between both organizations can make their assistance more focused and more effective.

The migration crisis of 2015–2016 in the Aegean Sea was not only a real test of the EU-NATO cooperation in emerging crises, but also an important and clear symbolism with serious impact on European public opinion on how the two organizations can face crises together. Seen as a "key test of relevance" for the Alliance, it led to NATO engaging its naval assets in patrolling the Aegean Sea, exchanging intelligence with the EU's FRONTEX through liaison officers. NATO also launched Operation SEA GUARDIAN and supported and still supporting, mainly with assets and intelligence, EUNAFORMED in the Central Mediterranean.

Any new development in their cooperation is a product of months of intense negotiations among the staff members, sometimes with the participation of some

MS and Allies and in some cases directly between involved national ministries. It can be said clearly, that it is the sense of urgency created by Hybrid and especially by Russian actions in Ukraine which created the existing impetus in the official EU-NATO relationship.

In order to counter Hybrid, NATO has been engaged in mostly unofficial talks with the EU, in four different areas:

- Civil-military planning
- Cyber Defense
- Information Sharing
- Strategic Communications

Although the frequency and the topic areas of staff-to-staff meetings have ups and downs, in general, they have grown both at political and expert levels, with the informal cooperation network being based mainly on personal and not institutional relations. The cooperation is considered as generally well-functioning.

Another aspect of this unofficial cooperation is linked to the Centers of Excellence (COE). The European Center of Excellence for Countering Hybrid Threats known also as “Hybrid COE,” is a network-based international and independent hub for practitioners and experts based in Helsinki, Finland. The Hybrid COE focuses on responses to hybrid threats under the auspices of the European Union (EU) and NATO [17].

Hybrid COE is described as a “do tank” that conducts training courses, exercises, hosts workshops to policymakers, and practitioners, and produces white papers on hybrid threats, such as vulnerabilities in an electrical grid or possible exploitation of vaguely written legislation. The Center was formally established in April 2017 inaugurated in October 2017 and is allotted a budget of 1.5 million euros. The Hybrid COE includes now 31 participating states of NATO and the EU, and has the potential to take a leading or at least a prominent position in this issue.

Since COEs have the advantage to cooperate with outside partners, they remain “half-in, half-out” of their institutional settings. The Finnish COE in order to accomplish its mission is allowed and able to cooperate with all the NATO COEs which deal with issues connected to Hybrid Threats, such as counterterrorism, cyber, piracy, CBRN, energy, etc. In addition, these connections have the potential to provide coordinated policy responses to both organizations, as long as this EU Center together with all the other relevant NATO Centers will avoid the trap of “*raising awareness from an academic point of view,*” and become clearly “operational” following the steps of the more “operational” NATO Cooperative Cyber Defense COE in Estonia [6].

Hybrid Warfare Concept has been around for more than 15 years gradually transforming and diffusing across the globe. The concept is based on the need to understand the changing character of society as well as of the conflict in recent decades. Although forms of what we call hybrid today, had implemented for centuries as well as during World Wars I and II and mainly during the Cold War, the changes in geopolitical landscape, society, and technology are the main reasons of the emergence of Hybrid Threats as a new global group of threats.



A number of newly emerged factors such as digitalization, globalization, the internet revolution, the emergence of social media as well the culturally increased social awareness and the ethnically diversification of the people, combined with reduced faith in authorities and senior public figures or political leaderships, all these factors have paved the way for this new kind of threats. By definition and nature, these threats challenge the traditional boundaries (political, bureaucratic, legal, and operational between military and civilian, public and private, national and collective capabilities) and already blurred the limits between war and peace.

There is no doubt that Hybrid Warfare has created confusion to the terminology of our vocabulary and should be seen as a manifestation of our inability to fit current security challenges within previously delineated logical terms for conceiving war. Hybrid is mainly the product of identification of self-diagnosed vulnerabilities as well the perceived enemy's new and surprised intentions. The Hybrid terms therefore deduced not only by "looking at the enemy" but also by "looking at the mirror," which led both EU and NATO to use Hybrid terminology in order to describe a changing security environment to which no clear policies existed. The need for a new concept was due to the realization that the so far well-known models of war and peace were not adequate to describe a rapidly evolving strategic international landscape. The Hybrid terms therefore are not about Russia, ISIS or weaponization of migration but rather seek to send a message of danger and urgency at a time of nominal peace. But the most important role of this modern terminology and of these patterns is to facilitate the communication to our decision-makers and to our population of all the challenges deriving from the new networked security environment, and the observed power diffusion.

As General Carl von Clausewitz said in probably his most oft-quoted passage, "*... the first, the supreme, the most far-reaching act of judgment that the statesman and commander have to make is to establish . . . the kind of war on which they are embarking.*" One cannot make this supreme judgment without a deep understanding of history, of war, and the various ways in which it is waged. Lacking that understanding increases the risk of mistaking the essential nature of the conflict being considered or those we must adapt to as a result of the ever-evolving character of warfare. The continuum concept and hybrid threats remain controversial since they distract from the efforts of "big wars" and great power competition advocates [2].

It is also important by using this Hybrid terminology to achieve the connection and the embodiment of Hybrid practices and modus operandi into the International Laws and Conventions institutional and Legal Architecture.

A particularly valid point is the need to consider the political dynamics of conflict, not just its methods or modes. This is not simply a statement of the obvious. It addresses a longstanding deficiency in the way war is perceived globally. "*Too often governments miss critical components of their adversary's strategy, typically because of a near-exclusive focus on its use of violence. Partial responses such as these can be counterproductive.*" This is the largest deficiency in hybrid threat theory; its emphasis on "how" the adversary applies violence overlooks the "why," which is ultimately more critical to counterstrategies and conflict [2].



Turning again to the two international organizations, while the EU deliberately chose the term “Hybrid Threats” over “Hybrid Warfare” mainly due to its civilian nature and in order to emphasize an “Integrated Approach” Policy, NATO used Hybrid Warfare to reinforce Allied solidarity and Alliance cohesion and to project stability outside its borders. Although both organizations avoided on purpose to make institutional or crucial changes to their internal processes and policy proposals, they were forced to push their adaptation programs toward the top of their agendas, showcasing their internal vulnerabilities and inadequacies *vis a vis* modern critical challenges and threats.

Concluding, the crises and conflicts of the twenty-first century reflect a greater degree of convergence and complexity and require from everyone to keep an informed and open mind on the various modes of conflict that already exist or are about to appear. In order to face our future security challenges, we need to reflect and interpret the past, understand the present, and think rigorously about what lies over the horizon in order to adapt to the challenging character of modern conflict [2].

Within this context, it is very important to have options available if the red lines are crossed, the thresholds are overpassed and the situation goes out of hand. These options should mainly include solid military capabilities that will save the day and support, defend, or impose your strategic goals. If things go the harm’s way, the Tweeter or Microsoft Navy or the Facebook or Apple Air Force (to copy Thomas L. Friedman) [18], is not capable enough and will not come to your rescue. Solid military capabilities and the political will to use them as appropriate, are often necessary to support your Hybrid Warfare activity.

There is no doubt that the Hybrid warfare is indeed the “today and tomorrow” of the Warfare. Decision-makers as well as civilian and military authorities and scholars have to study very well all aspects of Hybrid Warfare, without forgetting though, that negotiating “*with a loaded gun at your hand*” makes always a negotiation easier.

In addition, it is impossible to disregard the obvious benefit to our countries, of having the two organizations, NATO and the EU, working together on a so important issue as Hybrid Warfare. Hybrid intensified and facilitated the need of both organizations to come and work closer together for the protection of their role, their interests, their assets, and the protection of their citizens and their way of living.

## References

1. Walker, R.G.: Spec fi: The USMC and Special Operations. NPS (1998)
2. Hoffman, F.G.: Examining Complex Forms of Conflict, Gray Zone, and Hybrid Challenges. NDU/PRISM7 NO4 (2018)
3. Andersson, J.J., Tardy, T.: Hybrid: What’s in a name? EUISS, Brief Issue. (2015)
4. Hoffman, F.G.: Conflict in the Twenty-first Century: The rise of Hybrid Wars. Potomac Institute for Policy Studies (2007)

5. EEAS (2021) Documents on Countering Hybrid Threats
6. Uzieblo, J.J.: *United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats*. College of Europe (2017)
7. Galeotti, M.: The “Gerasimov Doctrine” and Russian Nonlinear War, In *Moscow Shadows*, (2014)
8. LGEN(ret) Ioannis Baltzois, *ISIS, and its Hybrid Warfare*, Hybrid Wars, Infognomon, 2022 (in Greek)
9. LCEN(ret) Ippokratis Daskalakis, *On Hybrid threats and wars*, Hybrid Wars, Infognomon, 2022 (in Greek)
10. [https://www.nato.int/cps/en/natohq/topics\\_156338.htm](https://www.nato.int/cps/en/natohq/topics_156338.htm)
11. European Commission & HR/VP: Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats, a European Union Response, p. 18. JOIN, Brussels (2016)
12. [https://www.nato.int/cps/en/natohq/official\\_texts\\_133163.htm](https://www.nato.int/cps/en/natohq/official_texts_133163.htm)
13. EPRS, Patryk Pawlak: *Countering hybrid threats: EU-NATO cooperation*, (2017)
14. European Commission & HR/VP, Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats, a European Union Response, Brussels, JOIN (2016) 18 final
15. EU Council Conclusions on the Integrated Approach to External Conflicts and Crises, 5413/18, 22 January 2018
16. [https://www.nato.int/cps/en/natohq/official\\_texts\\_133163.htm](https://www.nato.int/cps/en/natohq/official_texts_133163.htm) (Shared Vision, Common Action: A Stronger Europe)
17. <https://www.hybridcoe.fi/>
18. Friedman, T.L.: *A Manifesto for the Fast World*, New York Times Magazine, (1999)

# Hybrid Threats: A European Response



Dimitrios Anagnostakis

The concept of ‘hybrid threats’ has gained prominence during the last 10 years among the academia, military experts, states and governments and international organisations such as NATO and the European Union (EU). The European Union has developed a wide array of policies and tools that aim to strengthen its response and the response of its member states to a vast spectrum of hybrid threats. In parallel, several EU member states have developed their own policies, doctrines and tools designed to defend themselves from hybrid threats.

This proliferation of policy measures and institutional responses, that often leads to the problematic policy consistency and policy coherence, was to a large extent linked to two security issues that emerged in the early 2010s, namely the invasion of Crimea by Russia in 2014 and the resurgence of the threat of international terrorism exemplified in the early successes of the so-called Islamic State in Syria and Iraq [8] and the deadly attacks in Europe between 2014 and 2016. However, the concept of ‘hybrid war’ appeared much earlier, in particular in the early 2000s in discussions among military circles in the United States ([20]: 9). Even then, there were doubts about the usefulness of the term hybrid war; for many of its users, this term signified the combination of conventional and unconventional military means and tools, which as many critics highlighted was neither new nor unprecedented ([48]: 8).

Arguably, the main issue at stake is not whether the terms ‘hybrid threats’ and ‘hybrid war’ capture patterns of state and non-state behaviour that are entirely novel. What matters more is the undeniable fact that states and international organisations have already a long history of using these terms, which, therefore, should mean something for these states and organisations. In this chapter, I first take a brief look at

---

D. Anagnostakis (✉)  
University of Aberdeen, Aberdeen, UK  
e-mail: [dimitrios.anagnostakis@abdn.ac.uk](mailto:dimitrios.anagnostakis@abdn.ac.uk)

the hybrid terminology. Then I examine the EU response to hybrid threats focusing on the issues of situation and information awareness, the concept of resilience and the dimension of strategic communications as an exemplary case. Finally, I focus on the role of NATO and the EU-NATO relationship. While Europe has made significant progress in developing counter-hybrid policies during the last decade, issues such as the problematic policy implementation, the coherency and the overall coordination of the EU policies and sometimes the diverging priorities and threat perceptions of member states may hinder further progress in the future.

## 1 A Short History of the Hybrid Terminology

The three hybrid-related terms that are currently most in use are hybrid war, hybrid threats and hybrid conflict ([7, 39]: 47). Since the appearance of these terms in the early 2000s, both academics and the security and military professionals have fiercely debated whether these concepts are useful, whether they serve any meaningful purpose, whether the terms should be completely abandoned or replaced and of course about their novelty. The term hybrid war has the narrowest meaning among these three terms, and it has been the earliest to appear as mentioned above. Essentially, the term hybrid war was used to describe a military conflict where the enemy made a coordinated use of both conventional and unconventional military means. The burning policy issue at that time was how NATO and NATO members could adapt so that they would be able to respond to this kind of conflict. The original military posture of NATO was based on the assumption of a scenario of a conventional war against the Soviet Union and the Warsaw Pact. NATO's main mission and the ability of NATO to address the security threats challenging its members were cast into doubt first in the 1990s and then again in the early 2000s when the fight against terrorism emerged at the top of the political agenda for key member states such as the United States (US). One of the key events that shaped the debates about hybrid wars and conflicts in the 2000s was the war between Israel and Hezbollah in 2006 ([41, 46]: 96) which was perceived by many commentators as a defeat for Israel or at best a military stalemate, despite the heavy losses incurred upon Hezbollah.

Therefore, the terms hybrid wars and hybrid conflicts became the 'vehicles' through which security experts, military professionals and the military services and institutions of member states started sounding the alarm regarding NATO's urgent need for innovation. While the critics of the term noted that throughout the history of warfare, combatants have often made combined use of conventional and unconventional means [41], the individuals who stressed the novelty of hybrid highlighted that fast-pacing developments in the field of information and communication technologies and increased economic interdependencies have changed radically the security environment, thus the need for novel solutions [8].

## 2 The Response of the European Union

The first EU paper that addressed the issue of hybrid threats was the European External Action Service's (EEAS) paper titled 'Food-for-thought paper "Countering Hybrid Threats"' which was sent in 2015 to the member states' delegations. In that paper, rather than a clear definition, the EEAS essentially presented a list of hybrid characteristics. Hybrid warfare was described as follows:

' (...) A centrally designed and controlled use of various covert and overt tactics, enacted by military and/or non-military means, ranging from intelligence and cyber operations through economic pressure to the use of conventional forces. By employing hybrid tactics, the attacker seeks to undermine and destabilise an opponent by applying both coercive and subversive methods. The latter can include various forms of sabotage, disruption of communications and other services including energy supplies. (...) Massive disinformation campaigns designed to control the narrative are an important element of a hybrid campaign. All this is done with the objective of achieving political influence, even dominance over a country in support of an overall strategy' [17].

In the next year, the EU adopted its cornerstone framework for countering hybrid threats [9]; in that report 'hybrid warfare' is replaced by the term 'hybrid threats', though the definition remained essentially the same:

' (...) The concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare' [9].

Member states still have the main responsibility and competencies for responding to hybrid threats, as stressed in the EU's counter-hybrid framework [9]. However, the European Union has emerged as a facilitator and coordinator of the state responses. For example, intelligence and threat assessments shared by member states can be pooled together in the relevant EU bodies (e.g. the Hybrid Fusion Cell), which can then create all-source strategic reports or identify coordinated attacks against several states at the same time. Moreover, member states can benefit from the unique weight that the EU carries as a whole, especially in policy areas related to the common market and external trade (see, for example, the presence of economic sanctions in the 'Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities') ([5]: 9).

The rapid increase in the EU involvement in this field has followed the same pattern with the general increase of the EU involvement in the areas of internal security and Justice and Home Affairs in the post-9/11 years [1]. Repeated external shocks and crises such as the waves of terrorist attacks in Europe in the 2000s and the 2010s and the Russian invasions of Ukraine in 2014 and 2022 have driven home the realisation for the EU member states that it is difficult for them to address these threats alone and on their own; these shocks and crises worked as a 'window of opportunity' for those EU institutions and member states who were arguing for long time in favour of taking hybrid threats seriously ([22]: 6). The danger of such a crisis-driven policy response is of course that it can be difficult for the

EU to maintain a consistent momentum in the absence of new external crises, and, therefore, policy implementation problems may start to emerge.

Given that hybrid threats materialise across a variety of policy areas, the EU response to these threats spans similarly across different policy fields (e.g. cyber, economic, military, diplomatic, etc.). The depth and commitment of the EU response depend on the EU competencies and on the general progress that the EU has made over the previous years in developing policies for these fields. For instance, since the early 2010s, the EU has grown rapidly as an actor in the field of cybersecurity developing policies for the protection of critical information infrastructure and communication networks such as the NIS Directive, taking measures to increase the cyber resilience of member states and enhancing the EU institutions and actors which are responsible for these policy issues (e.g. the European Union Agency for Cybersecurity ENISA or the European Cybercrime Centre in Europol) ([2]: 246). Therefore, when the issue of hybrid threats appeared in the political agenda in the 2010s, the EU had already started focusing on cybersecurity and cyber resiliency which form part of the overall defence against hybrid threats. The key issue has been and continues to be not so much how to formulate entirely new policies—there are already existing strategies and sectoral policies on foreign and security policy, defence, energy security, maritime security, etc.—but rather to ‘facilitate a holistic approach (...) by creating synergies between all relevant instruments and fostering close cooperation between all relevant actors’ ([9]: 3).

In July 2020, the Commission published a document mapping the hybrid threats-related measures that have been taken at the EU level [15]. According to this inventory, more than two hundred measures related to countering hybrid threats have been initiated, most of them in the period after the adoption of the EU Joint Framework for Countering Hybrid Threats in 2016. These measures relate to the following policy fields: strategic communications and countering disinformation, promoting EU common values and inclusive, open and resilient societies, protection of critical infrastructure, the energy sector, screening of foreign direct investments, the transport sector, the space sector, border controls, defence capabilities and the Common Security and Defence Policy, civil protection, public health, addressing chemical, biological, radiological and nuclear-related risks, cybersecurity, the financial sector, cooperation with third countries and with NATO, preventing, responding to crisis and recovering and finally the EU’s institutional resilience. Since 2020, the EU has kept up with this pace adopting additional measures in various policy fields.

## ***2.1 Situation and Information Awareness***

Irrespective of the policy instrument or instruments used by the adversary, it is essential for the country defending against hybrid threats to have a full picture of the unfolding enemy campaign. The EU has often stressed that it is crucial for itself and for its member states to be able to recognise coordinated hybrid attacks that target

more than one member state. For this to happen, however, member states should be willing to share information and intelligence in real time with the relevant EU agencies and institutions and among themselves ([10]: 9). In other words, the EU is uniquely positioned to function as an ‘one-stop’ point for receiving intelligence and information related to emerging hybrid threats or developing hybrid attacks, for producing situation awareness and all-source strategic reports based on this information and for illuminating the threat environment for member states.

The EU’s Hybrid Fusion Cell—which is based within the EU’s intelligence unit called the EU Intelligence Analysis Centre (formerly called EU Situation Centre)—has exactly this role of collating information related to hybrid threats, monitoring the EU’s security and threat environment and producing a series of intelligence reports, including threat analyses and all-source strategic reports. Apart from the information voluntarily shared by member states, the Cell also collects information from other EU institutions and from the EEAS delegations around the world ([11]: 2) and it is also in contact with NATO’s Hybrid Analysis Branch.

In practice, however, the issue of implementation, which has often beset EU initiatives and policies in the past, ‘holds back’ the Hybrid Fusion Cell. Similarly to what happens in other policy areas, such as counterterrorism or cybersecurity where the EU institutions rely largely on the voluntary contributions and cooperation of member states for raw information and for intelligence products, not all member states are equally willing to share information with the Cell. Every time there is a geopolitical crisis or a major security threat, practitioners, experts, and policymakers start calling for the need to strengthen intelligence cooperation at the EU level or even for the creation of a ‘real’ EU intelligence agency which will have the ability to collect operational information ([37]: 483). However urgent these crises are, member states are still not willing to trust all their partners equally; sharing intelligence with an EU body or institution often translates into making this information available to all 27 EU member states. Deepened multilateral intelligence cooperation is more often seen among smaller groups of states or bilaterally and it is usually structured at an ad hoc basis rather than permanently institutionalised [25].

Apart from the states, private non-state actors have also a role to play in creating an environment of situation and information awareness regarding hybrid threats and attacks ([47]: 88; [49]: 25). The spectrum of hybrid threats includes, among others, cyberattacks against banks and financial institutions and disinformation campaigns with fake or distorted stories and narratives carefully planted in social media or even in traditional media ([20]: 27). As mentioned above, two key issues in defending against hybrid attacks are first identifying these attacks early and second identifying hybrid attacks as such, namely not as isolated incidents but as coordinated campaigns aiming to destabilise societies and states. For this to happen, however, and so that both member states and the EU are able to connect the dots and see the larger picture, there should be, for instance, a reporting process through which the companies which are victims of cyberattacks or cyber incidents can report

them.<sup>1</sup> Similarly, fighting against disinformation and fake news requires that there is in place a process of collecting pieces of disinformation and reporting them on a dedicated platform as well as a process of trying to identify common patterns and coordinated adversarial campaigns.

However, private actors have been traditionally very reluctant to share information about cyberattacks and cyber incidents or to take any measures to curb the proliferation of fake news or to strengthen their vigilance against disinformation campaigns. The primary motivation for these actors is profit, and sharing information about their vulnerabilities can potentially affect their customers' views and thus their market share and profits. The EU's Network and Information Systems (NIS) Directive stipulates that it is compulsory for critical infrastructure operators to report and disclose to national authorities any cyber incident or breach that has a significant impact on their operations. However, this regulation has been criticised by security professionals for being too timid; it does not cover, for instance, the reporting of security vulnerabilities or the very big companies which, despite their size, are not perceived as providing critical services [45]. The Directive has been the product of prolonged negotiations and bargaining among member states with the end result being that national authorities have a lot of flexibility in how they implement it. A second NIS Directive is currently under negotiations; the Council and the Commission have come to a political agreement and the European Parliament is expected to decide on the issue by the end of 2022 [36].

## ***2.2 Defending Against Hybrid Threats and Mitigating Against Their Impact Through Resilience***

Resilience is the 'buzzword' that summarises the EU's approach in defending against hybrid threats and mitigating against their impact. Building resilience means that state institutions and societies can withstand, for instance, disinformation campaigns, attacks against critical infrastructure, border pressure from increased migrant flows weaponised and coordinated by adversaries and economic pressure and the exploitation of economic and energy interdependencies [6]. The concept of resilience is not new within the EU, as it first emerged in the issue area of cybersecurity when cyber resilience became an umbrella term covering topics such as the protection of critical information infrastructure, reducing cybercrime and its economic impact and enhancing the cybersecurity standards in the private sector ([10]: 3).

The concept of societal resilience as a broad line of defence against hybrid threats is related to another conceptual framework that is often mentioned in policy documents, namely the whole-of-government [10] or whole-of-society [16]

---

<sup>1</sup> The EU's Network and Information Systems Directive includes a compulsory requirement for reporting major cyber breaches but this applies only to critical infrastructure operators.



approach. While the whole-of-government concept reflects the key idea that hybrid threats span across a range of different policy areas, the whole-of-society concept highlights the elevated role that non-state actors and individual citizens can play in countering hybrid threats ([24]: 15). For example, the private sector is encouraged to adopt stronger cybersecurity standards so that it can withstand cyberattacks. In another example, media literacy among citizens is crucial for remaining unaffected from disinformation campaigns [34]. Academia, research centres and think tanks have also a role to play by conducting research on all the topics that relate to hybrid threats and the defence against them. More broadly, if one of the defining characteristics of hybrid campaigns is that they specifically target ‘the systemic vulnerabilities in democratic societies’ ([20]: 11), by exploiting, for instance, social and political cleavages and making a malign use of the free press in order to undermine democracy, then ultimately the best defence is nourishing the public’s trust in democratic institutions ([49]: 24).

For instance, Esther Brimmer has noted in her discussion of the term ‘homeland security’, which was popular in the post-9/11 years, that during the last decades the concept of security has evolved: security is not only about defending territories but also about protecting ‘the values, connections and infrastructure [that characterise] the modern globalised world’ ([4]: 29). Brimmer was thus arguing in favour of a holistic approach to security as early as in 2006. A holistic approach, or, as she names it, ‘societal security’, includes not only efforts to prevent enemy attacks, to reduce vulnerabilities and to minimise the consequences if attacks occur but also the respect for and the protection of societal values such as the rule of law and civil liberties. In particular, societal security consists of two elements: cohesion and physical protection ([4]: 31). Cohesion includes the values that characterise and bind a society: democracy, rule of law and civil liberties, education, welfare and pluralism. Physical protection includes infrastructure, public health, natural disaster relief, environmental quality and anti-terrorism measures. Therefore, Brimmer was arguing that homeland security can fit within the broader schema of societal security, as it contains components from both elements of societal security, as defined by her. Arguably, the concept of societal security can enrich the discussion about the manifestation of hybrid threats and the defences that one can raise against them, as the EU keeps stressing that these threats often seek ‘to undermine fundamental democratic values and liberties’ [9] or to ‘destabilise countries by undermining public trust in government institutions and challenging the core values of societies’ [10].

In the following section, I am focusing on a particular dimension of hybrid threats and the defence against them: disinformation, malign narratives and fake news. This case study is illuminating with regard to the EU response to hybrid threats as, contrary to other policy fields such as cybersecurity, here the EU had to build its counter-hybrid policies ‘from scratch’.

### 2.3 *Strategic Communications and the Fight Against Disinformation*

Before the EU published its first communication on countering hybrid threats in 2016, it had already created a strategic communications cell within the External Action Service: the ‘East StratCom Task Force’ was established in 2015 in the wake of the Russian invasion in Crimea and the increased Russian efforts to spread disinformation and fake news about Ukraine among European audiences ([22]: 38). The ‘Arab StratCom Task Force’ was established in the same year focusing on countering radicalisation in the Arab world (contrary to the East StratCom, this task force did not have its own dedicated staff) [29]. Additional StratCom teams were established in 2016 focusing on the countries in the Middle East and Northern Africa and the Gulf region (‘Task Force South’) and the Western Balkans (‘Western Balkans Task Force’) [12]. All these teams were placed under a Strategic Communications Division within EEAS.

The creation of Task Force South was related to the rise of the so-called Islamic State group which made a very effective use of propaganda, online recruitment and social media. While very different in scope, the online activities of both the Islamic State and the Russian government in the field of communications were perceived as having ultimately the same effect: undermining trust in democratic institutions and destabilising societies, undermining in other words the resilience of European societies [17]. Moreover, in both cases the elements of propaganda and disinformation were accompanied by a variety of other actions located throughout the whole spectrum of hybrid threats: for instance, the Islamic State combined the use of intensive online propaganda and recruitment with the use of both conventional and guerilla tactics in the battlegrounds in Syria and Iraq.

Disinformation is defined by the EU as follows:

‘Disinformation is understood as verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Public harm comprises threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens’ health, the environment or security. Disinformation does not include reporting errors, satire and parody, or clearly identified partisan news and commentary.’ ([13]: 3–4).

According to this definition, disinformation is different from propaganda which aims at creating a positive image for the disseminator. Moreover, the EU documents on disinformation have repeatedly stressed that even harmful content is often legal—in that case it is protected by freedom of expression—and it ‘needs to be addressed differently than illegal content, where removal of the content itself may be justified’ ([13]: 1). Examples of illegal content that are out of the scope of counter-disinformation policies include the dissemination of election-related materials when that dissemination violates electoral laws or terrorist content/materials published online.

As early as 2015, the strategic communications action plan of the Commission for the Eastern neighbourhood envisioned three main pillars: (1) building and

disseminating positive narratives and stories about the EU policies and initiatives; (2) strengthening the media environment and media freedom; (3) exposing false information and fake news and building awareness regarding disinformation [18]. In its 2018 communication on tackling online disinformation, the EU followed along similar lines, focusing on improving transparency about the origin, production and dissemination of information, enhancing media literacy and supporting high-quality journalism, creating a network of fact-checkers, authenticators, and trusted ‘flaggers’ and creating a multi-stakeholder model where all relevant parties (e.g. governments, the private sector, social media platforms, academia, etc.) participate and take responsibility [13]. Essentially, the EU approach reflects what was mentioned above regarding the need for effective situation awareness, an emphasis on societal resilience and a whole-of-society perspective. This communication was accompanied by an ‘Action Plan against Disinformation’ which gave more details about the specific EU aims in that field [12]. One of the key actions of the plan was the creation of a Rapid Alert System designed to provide alerts on disinformation campaigns in real time. The rapid alert system would receive information and alerts from member states through national contact points and it would also be linked with other information and crisis monitoring networks of the EU, such as the Emergency Response Coordination Centre and the Situation Room and the EU Hybrid Fusion Cell within EEAS. Moreover, the 2018 Action Plan suggested the strengthening of the budget, capacities, personnel and training of all the strategic communications teams working within EEAS, highlighted the importance of the 2018 EU Code of Practice on Disinformation, and stressed the importance of safeguarding the 2019 European Parliament elections from foreign interference.

At the moment of writing, the Strategic Communications Division has a stronger presence within EEAS and a broader mandate compared to 2015. The division now has several work strands and priorities: ‘pro-active communication and awareness raising, support to independent media and the detection, analysis and challenge of information manipulation and interference activities by foreign states’ ([19]: 5). In broader terms, and with regard to the EU’s overall framework for countering hybrid threats, the division’s work spans across four dimensions: situational awareness, resilience building, disruption and regulatory approaches and diplomatic responses or CFSP responses ([19]: 5).

In practice, there are several initiatives that have worked well and are considered a success. One of them is the division’s ‘EU vs. Disinfo’ website and social media accounts, which is promoted as a ‘flagship’ initiative by EEAS. It was originally created in 2015 as a tool for monitoring, countering and debunking Russian disinformation campaigns. In terms of its role in the EU’s framework for countering hybrid threats, it contributes to strengthening the resilience of the public and raising awareness about the malicious disinformation activities of foreign actors ([19]: 9). The EU vs. Disinfo database currently includes 14,377 pieces written in various languages and collected mostly from pro-Russian media outlets. Apart from a focus on Russia and Ukraine, the database has also special thematic sections on Belarus, China and COVID-related disinformation.

A second initiative that has created positive momentum in fighting disinformation is the 2018 EU Code of Practice on Disinformation which was launched ahead of the European Parliament Elections in 2019. Given the previous examples of electoral interference in the 2016 US presidential elections, the EU was anxious about similar meddling with its own elections. The EU's code of practice on disinformation was, therefore, an effort by the Union to encourage key companies to self-regulate themselves by implementing a series of best practices: the companies which signed the code (including Facebook, Twitter, Mozilla and Google) pledged to build more transparency and visibility about paid political advertising, to be swifter in taking down fake accounts and to end support and monetisation for disseminators of disinformation [14, 44].<sup>2</sup>

Finally, the cooperation of the EEAS' Strategic Communications Division with third partners and its general 'outwards' institutional engagement can be considered as a success. For instance, the division maintains regular contact with NATO, the NATO's Centre of Excellence on Strategic Communications in Riga and the European Centre of Excellence for Countering Hybrid Threats in Helsinki.

Less progress has been made, however, in other areas. Arguably, the Rapid Alert System has not been utilised to its full potential by the EU member states. Ultimately, this reflects some of the perennial problems that all EU initiatives in security-related areas face: lack of prioritisation regarding this policy area by some states and/or lack of trust.

### 3 The Response of NATO and the EU-NATO Cooperation

Compared to the EU, the concepts of 'hybrid threats' and 'hybrid war' appeared earlier in NATO. As early as 2010, NATO's Bilateral Strategic Command (Bi-SC) published its 'Input for a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats' [33]. This paper highlighted three themes: the emergence of new threats 'which potentially have grown beyond the current remit' of NATO, the blurring of the dividing line between military and civilian responsibilities under a changing security environment and the need for NATO to strengthen and make more use of its partnerships and to significantly expand its cooperation with third parties 'beyond its borders' ([33]: 2). It also defined hybrid threats as the threats posed by adversaries who 'simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives'.

While NATO in general has preferred to talk about 'hybrid war' rather than about 'hybrid threats', which is the preferred term for the EU, the authors of this paper acknowledge the variety of forms in which these threats materialise: 'hybrid threats are comprised of, and operate across, multiple systems/subsystems (including

---

<sup>2</sup> The code has been updated in 2022.

economic/financial, legal, political, social and military/security) simultaneously and will therefore prove problematic for NATO's response which would initially focus upon a military/security line of operation' ([33]: 4). This acknowledgement reflects a general anxiety within NATO about the role of the Alliance in the post-Cold War era. Similar questions about the adaptability of NATO to new security challenges were raised repeatedly in the 1990s and in the context of the post-9/11 'War on Terror'.

In parallel to the EU developments, the debates within NATO focused on the 'comprehensive approach' to security and how it can be adapted for countering hybrid threats and on the concept of resilience ([40]: 4). However, these debates were not always smooth as not all NATO members agreed about either the importance or novelty of hybrid threats or about how these threats should be defined and conceptualised ([48]: 15). Similarly, however, with how a series of consecutive external crises and shocks (the cyberattacks against Estonia in 2007, the 2008 Russian-Georgian war, the war in Ukraine in 2014 and the rise of the Islamic State in 2014) changed the calculations among the EU member states, the same events were also a wake-up call for NATO and its members ([26]: 271).

Regarding the dimension of information and awareness, NATO has adapted to the new security challenge of hybrid threats by reorganising its intelligence bodies. In 2017, the 'Joint Intelligence and Security Division' was established by fusing together civilian and military intelligence [28]. In the same year, a Hybrid Analysis Branch was created within this new division focusing on analysing information from both civilian and military sources; the ultimate aim was 'connecting the dots' and creating a holistic picture and understanding of the hybrid threat landscape [43]. A key pillar of the EU-NATO cooperation on countering hybrid threats is the relationship and close cooperation between the EU's Hybrid Fusion Cell and NATO's Hybrid Analysis Branch; this cooperation was significantly enhanced after the 2016 Joint EU-NATO Declaration in Warsaw which ushered a new period in the relations between NATO and the EU. Regarding cyber defence in particular, NATO has often stressed that swift information-sharing about cyber incidents is an essential element in improving the cyber resilience of allies.

In terms of NATO's defence against hybrid threats, one key development has been NATO's public announcement in 2016 that the article five of its founding treaty regarding collective defence is applicable in cases where there is a hybrid threat or attack against an ally [31]; the same was repeated in 2021 [32]. This was an essential step for the reassurance of the members who felt particularly threatened from Russia in the post-2014 security environment. However, one of the unique characteristics of hybrid threats and hybrid escalation is that the attribution of the exact source of threats and attacks is often difficult—states seek to retain plausible deniability—and at the same time NATO and its member states need detailed protocols and operational 'playbooks' for responding to acts that fall short

of open military attack/aggression ([26]: 270). This problem has been extensively discussed, for instance, in the context of cyberattacks and cyber defence [42].<sup>3</sup>

Apart from the diplomatic posture and signalling regarding article five and the possibility of triggering it if a member is the victim of a hybrid attack, NATO has significantly enhanced its collective defence capabilities since 2014 ([26]: 271). The Readiness Action Plan which was adopted in 2014 included measures focusing on both military adaptation, including adapting to hybrid threats, and on the assurance of allies through ‘continuous air, land and maritime presence and meaningful military activity in the eastern part of the Alliance’ [30]. In this context, a strategy on NATO’s role in countering hybrid warfare was adopted in 2015 [31] and in 2018 NATO agreed to set up counter-hybrid support teams; these teams support and assist NATO members in building resilience and in defending or responding to hybrid threats. The first such team was deployed in Montenegro to assist the country in detecting and mitigating vulnerabilities and in enhancing its resilience [43].

Regarding the dimension of strategic communications, similarly with the EU NATO started being preoccupied with this issue in 2014. In that year, seven NATO members (Latvia, Estonia, Germany, Italy, Lithuania, Poland and the United Kingdom) established in Riga, the NATO Strategic Communications Centre of Excellence (NATO StratCom COE). The mission of this centre, which is not officially tied to the NATO command, is to assist and support the NATO member states and their allies in issues related to strategic communications, including, for instance, countering disinformation and producing counter-narratives, running exercises and scenarios related to strategic communications, engaging in academic research and contribution to doctrine development, among others ([35]: 3). In these activities, the Centre cooperates closely with the EU’s Strategic Communications Division within EEAS but also with third actors, such as academia and the private sector.

### ***3.1 The EU-NATO Cooperation***

The relationship between the EU and NATO has been especially enhanced and prioritised since the 2016 EU-NATO Joint Declaration in the Warsaw Summit. Even before 2016, however, there was a realisation among NATO circles that the new security challenges, including hybrid threats, require that the Alliance cooperates more closely with other international organisations, including the EU. The 2010 ‘Input for a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats’ warned, for instance, that these challenges have a strong civilian element for which NATO was not well prepared, making thus

---

<sup>3</sup> For a thoughtful analysis on the classical deterrence model and its applicability to the hybrid threat environment, see Rasmus Hindrén’s working paper ‘Calibrating the compass: Hybrid threats and the EU’s Strategic Compass’ [23].

cooperation with third partners essential. Despite the debates in both academia and policymakers about friction between the EU and NATO regarding their ‘division of labour’ in the post-Cold War environment, the EU’s strong civilian element with established policies in hybrid threats-related areas (ranging from trade and economic sanctions to cyber resilience and the protection of critical infrastructure) made it especially attractive to NATO ([3]: 22). In 2016, the two organisations committed themselves, as a result, in implementing a series of actions and measures for countering hybrid threats. The measures and actions agreed are updated yearly and they are accompanied by yearly implementation reports.

In particular, in the area of situation and information awareness, the EU’s Hybrid Fusion Cell and NATO’s Hybrid Analysis Branch meet at least once a month, ‘with the aim of strengthening situational awareness and mutual understanding of respective activities’ [21]. The aim is to have a common picture with regard to the hybrid threats landscape and to be able to exchange information swiftly when there is an escalating crisis. The form that this ‘common picture’ takes is the joint EU-NATO documents ‘Parallel and Coordinated Assessments’; three such reports were published, for instance, between June 2020 and May 2021 [21]. The same staff also make frequent contributions to the joint EU-NATO exercises, such as the Parallel and Coordinated Exercises (PACE) [27].

Regarding strategic communications, this is another area where there is significant cooperation between the relevant staff of the two organisations. The issues that are being discussed cover enhancing the resilience of societies in the face of disinformation campaigns and fake news, exchanging best practices for identifying and countering disinformation campaigns and for building positive counter-narratives and supporting the members of NATO and the EU with policy templates and policy guides and training materials related to strategic communications. The strategic communications teams from both sides also test their capacity to formulate common narratives and messaging during joint EU-NATO exercises. Moreover, the NATO Strategic Communications Centre of Excellence also maintains close ties with the EU’s EEAS Strategic Communications Division; the two sides produced in 2020 a training course for EU staff which simulates disinformation attacks and responses [21]. In the same year, NATO staff was included in the EU’s Rapid Alert System which provides a platform for sharing and exchanging information on disinformation incidents and campaigns. Finally, more recently the two organisations have participated in discussions on COVID-related disinformation and its impact on the resilience of member states.

Apart from strategic communications, the scope of the staff-to-staff contacts and discussions has gradually increased covering areas such as minimum requirements for the resilience of critical infrastructure, providing rapid support to allies to support their resilience, civil preparedness and mitigating the impact of Chemical, Biological, Radiological and Nuclear (CBRN) threats. Moreover, the European Centre for European Centre of Excellence for Countering Hybrid Threats in Helsinki, which was established in 2017 by a number of NATO and EU members, plays a crucial role in supporting the EU-NATO relationship in that field and in assisting the two organisations and its members in understanding and responding to



hybrid threats. For instance, in 2020 a joint report was published by the European Centre for European Centre of Excellence for Countering Hybrid Threats and the NATO Strategic Communications Centre of Excellence about how to attribute information influence operations and how to identify those responsible for such operations [38].

## 4 Conclusion and the Way Ahead

In conclusion, it can be argued that Europe has made significant progress in developing counter-hybrid policies during the last decade and especially in the period after the Russian invasion of Crimea in 2014. Evidence of this progress can be seen in the swiftness by which both NATO and the EU responded to the renewed invasion of Ukraine by Russia in February 2022; the common messaging of the two organisations and their overall coordination of their actions were often tested in previous tabletop exercises simulating similar scenarios. In general, an almost permanent feature of EU history is that policy development, institutional strength and policy integration at the EU level originate through exogenous crises and shocks.

The question that this observation raises, though, is whether this policy momentum is sustainable in the long-term, especially if one considers the often-diverse threat perceptions of member states. Finland has been one of the countries that played an active role in shaping the response and the policies of the EU in the 2010s and especially after 2014 ([47]: 83). Not all EU member states shared, however, at that time the Finnish argument that the fight against hybrid threats should be dealt at an EU level or even the view that this issue should at least be addressed at a national level. Ultimately, the crisis of 2014 and the subsequent change in the European security environment as well as the proactive stance of the Commission and the EEAS on that field meant that eventually compromises were built among the EU member states resulting thus in the emergence of an EU response. The different threat perceptions and the different levels of prioritisation are currently reflected in the varied willingness of the EU member states to use or support and bolster the existing mechanisms and institutions focusing on countering hybrid threats.

In general, the multi-level governance of the EU, combined with the nature of hybrid threats, means that a number of actors at various levels and from different policy areas—state actors, state militaries, EU institutions and bodies, private companies, economists, IT professionals, law enforcement officials, etc. — are responsible each time for planning and implementing the counter-hybrid policies across the whole spectrum of hybrid threats. This fragmented policy landscape raises obvious issues of policy coherence and policy consistency. In the post-9/11 period and with regard to the EU counter-terrorism response, the EU established the position of an EU counter-terrorism coordinator, partially in order to solve similar issues; it would not be surprising, therefore, to see calls for the establishment a similar role for coordinating the overall counter-hybrid EU effort.



Essentially, both NATO and the EU acknowledge repeatedly in their various strategies and reports that member states have the primary responsibility for responding to hybrid attacks. Therefore, any further progress in policy development and cooperation at the EU level will partially depend upon the willingness of the EU members to make use of the existing mechanisms at this level. One way through which the EU could enlist more support from member states in the future could be by emphasising even more the concept of societal resilience and a whole-of-society approach as guides for countering hybrid threats and by assisting states in building their own counter-hybrid strategies; ultimately, by building societal resilience as a means of defending against such threats states also create defences for a broad array of contemporary challenges that move beyond the confines of hybrid attacks.

## References

1. Anagnostakis, D.: *EU-US Cooperation on Internal Security: Building a Transatlantic Regime*. Routledge, London (2017)
2. Anagnostakis, D.: The European Union-United States cybersecurity relationship: a transatlantic functional cooperation. *J. Cyber Policy*. 6(2), 243–261 (2021)
3. Argano, M.E.: NATO's effective multilateralism: the means to counter hybrid threats. (2018). Retrieved September 20, 2022, <https://www.ndc.nato.int/news/news.php?icode=1202>
4. Brimmer, E.: From territorial security to societal security: implications for the transatlantic strategic outlook. In: Brimmer, E. (ed.) *Transforming Homeland Security: U.S. and European Approaches*, pp. 23–42. The John Hopkins University, Washington, D.C. (2006)
5. Council of the EU. Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – approval of the final text. Brussels, 09/10/2017, 3007/17 (2017)
6. Council of the EU. Complementary efforts to enhance resilience and counter hybrid threats - council conclusions (10 December 2019). Brussels, 10/12/2019, 14972/19 (2019)
7. Cullen, P.: A perspective on EU hybrid threat early warning efforts. In: Weissmann, M., Nilsson, N., Palmertz, B., Thunholm, P. (eds.) *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, pp. 46–57. I. B. Tauris, London (2021)
8. Drent, M., Hendriks, R., Zandee, D.: *New Threats, New EU and NATO Responses*. Clingendael Institute, The Hague (2015)
9. European Commission. Joint framework on countering hybrid threats: a European response. Brussels, 06/04/2016, JOIN (2016) 18 final (2016)
10. European Commission. Increasing resilience and bolstering capabilities to address hybrid threats. Brussels, 13/06/2018, JOIN (2018) 16 final (2018a)
11. European Commission. Implementation of the joint framework on countering hybrid threats from July 2017 to June 2018. Brussels, 13/06/2018, JOIN (2018) 14 final (2018b)
12. European Commission. Action plan against disinformation. Brussels, 05/12/2018, JOIN (2018) 36 final (2018c)
13. European Commission. Tackling online disinformation: a European approach. Brussels, 26/04/2018, COM (2018) 236 final (2018d)
14. European Commission. Questions and answers – code of practice against disinformation: commission calls on signatories to intensify their efforts. Brussels, 29/01/2019, MEMO/19/752 (2019)
15. European Commission. Mapping of measures related to enhancing resilience and countering hybrid threats. Brussels, 24/07/2020, SWD (2020) 152 final (2020)

16. European Commission. Second Progress report on the implementation of the EU security union strategy. Brussels, 23/06/2021, COM (2021) 440 final (2021)
17. European External Action Service. Food-for-thought paper “Countering Hybrid Threats”. Brussels, 13/05/2015, EEAS (2015) 731 (2015a)
18. European External Action Service. Action Plan on Strategic Communication. Brussels, 22/06/2015, Ref. Ares (2015) 2608242 (2015b)
19. European External Action Service. 2021 StratCom activity report - Strategic Communication Task Forces and Information Analysis Division. (2021). Retrieved September 20, 2022, from [https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-and-information-analysis\\_en](https://www.eeas.europa.eu/eeas/2021-stratcom-activity-report-strategic-communication-task-forces-and-information-analysis_en)
20. European Union & Hybrid CoE. (2020). The Landscape of Hybrid Threats: A Conceptual Model Public Version. (2021). Retrieved September 20, 2022, from <https://op.europa.eu/en/publication-detail/-/publication/b534e5b3-7268-11eb-9ac9-01aa75ed71a1/language-en>
21. EU-NATO. EU- NATO cooperation: sixth progress report. (2021). Retrieved September 20, 2022, from <https://www.consilium.europa.eu/en/press/press-releases/2021/06/03/eu-nato-cooperation-sixth-progress-report/>
22. Fiott, D., Parkes, R.: Protecting Europe: The EU’s response to hybrid threats. (2019). Retrieved September 20, 2022, from <https://www.iss.europa.eu/content/protecting-europe-0>
23. Hindrén, R.: Hybrid CoE Working Paper 12: Calibrating the compass: Hybrid threats and the EU’s Strategic Compass. (2021). Retrieved September 20, 2022, from <https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-12-calibrating-the-compass-hybrid-threats-and-the-eus-strategic-compass>
24. Kremidas-Courtney, C.: It’s all about governance: addressing hybrid and transnational threats. In: André, I., Arenella, R. (eds.) Hybrid and Transnational Threats, pp. 13–16. Friends of Europe, Brussels (2018)
25. Labasque, N.: The merits of informality in bilateral and multilateral cooperation. *Int. J. Intell. CounterIntell.* **33**(3), 492–498 (2020)
26. Lasconjarias, G., Jacobs, A.: NATO’s hybrid flanks: handling unconventional warfare in the south and the east. In: Lasconjarias, G., Larsen, J.A. (eds.) NATO’s Response to Hybrid Threats, pp. 257–276. Nato Defense College, Rome (2015)
27. Latici, T.: Understanding EU-NATO cooperation: Theory and practice. (2020). Retrieved September 20, 2022, from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659269/EPRS\\_BRI\(2020\)659269\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/659269/EPRS_BRI(2020)659269_EN.pdf)
28. von Loringhoven, A.F.: Adapting NATO intelligence in support of “One NATO”. (2017). Retrieved September 20, 2022, from <https://www.nato.int/docu/review/articles/2017/09/08/adapting-nato-intelligence-in-support-of-one-nato/index.html>
29. Missiroli, A., Gaub, F., Popescu, N., Wilkins, J.-J.: Strategic communications: East and South. (2016). Retrieved September 18, 2022, from <https://www.robert-schuman.eu/en/european-issues/0415-strategic-communications-east-and-south>
30. NATO. Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. (2014). Retrieved September 20, 2022, from [https://www.nato.int/cps/en/natohq/official\\_texts\\_112964.htm](https://www.nato.int/cps/en/natohq/official_texts_112964.htm)
31. NATO. Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016. (2016). Retrieved September 20, 2022, from [https://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm](https://www.nato.int/cps/en/natohq/official_texts_133169.htm)
32. NATO. Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021. (2021). Retrieved September 20, 2022, from [https://www.nato.int/cps/en/natohq/news\\_185000.htm](https://www.nato.int/cps/en/natohq/news_185000.htm)
33. NATO Bi-SC. Input for a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Threats. (2010). Retrieved September 20, 2022, from [https://www.act.nato.int/images/stories/events/2010/20100826\\_bi-sc\\_cht.pdf](https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf)
34. NATO StratCom COE. Strategic Communications Hybrid Threats Toolkit. (2021a). Retrieved September 18, 2022, from <https://stratcomcoe.org/publications/strategic-communications-hybrid-threats-toolkit/213>

35. NATO StratCom COE. Annual Report. (2021b). Retrieved September 18, 2022, from [https://stratcomcoe.org/uploads/Gada%20Parskati/Annual\\_report\\_2020\\_audited\\_upd\\_8.pdf](https://stratcomcoe.org/uploads/Gada%20Parskati/Annual_report_2020_audited_upd_8.pdf)
36. Negreiro, M.: The NIS2 Directive: A high common level of cybersecurity in the EU. (2022). Retrieved September 20, 2022, from [https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS\\_BRI\(2021\)689333\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf)
37. Palacios, J.-M.: On the road to a European intelligence agency? *Int. J. Intell. CounterIntell.* **33**(3), 483–491 (2020)
38. Pament, J., Smith, V.: *Attributing Information Influence Operations: Identifying Those Responsible for Malicious Behaviour Online.* (2022). Retrieved September 20, 2022, from <https://stratcomcoe.org/publications/attributing-information-influence-operations-identifying-those-responsible-for-malicious-behaviour-online/244>
39. Pawlak, P.: *Understanding Hybrid Threats.* European Parliamentary Research Service, Brussels (2015)
40. Pawlak, P.: *Countering Hybrid Threats: EU-NATO Cooperation.* European Parliamentary Research Service, Brussels (2017)
41. Popescu, N.: *Hybrid Tactics: neither new nor only Russian.* (2015). Retrieved September 20, 2022, from <https://www.iss.europa.eu/content/hybrid-tactics-neither-new-nor-only-russian>
42. Prucková, M.: *Cyber attacks and Article 5 – a note on a blurry but consistent position of NATO.* (2022). Retrieved September 20, 2022, from <https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/>
43. Rühle, M., Roberts, C.: *Enlarging NATO’s toolbox to counter hybrid threats.* (2021). Retrieved September 20, 2022, from <https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html>
44. Tanner, B.: *EU Code of Practice on Disinformation.* (2022). Retrieved September 20, 2022, from <https://www.brookings.edu/blog/techtank/2022/08/05/eu-code-of-practice-on-disinformation/>
45. Tech Monitor. *Cyber incident reporting rules aren’t working. Can the UK fix them on its own?* (2021). Retrieved September 20, 2022, from <https://techmonitor.ai/technology/cybersecurity/cyber-incident-reporting-rules-arent-working-can-the-uk-fix-them-on-its-own>
46. Tenenbaum, É.: *Hybrid warfare in the strategic spectrum: an historical assessment.* In: Lasconjarias, G., Larsen, J.A. (eds.) *NATO’s Response to Hybrid Threats*, pp. 95–112. Nato Defense College, Rome (2015)
47. Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K., McCue, M.: *Addressing Hybrid Threats.* Swedish Defence University, Stockholm (2018)
48. Uziębło, J.J.: *United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats.* College of Europe, Bruges (2017)
49. Wigell, M., Mikkola, H., Juntunen, T.: *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats.* European Parliament, Directorate-General for External Policies, Policy Department, Brussels (2021)

# Integrated Development Environment Using M&S and AI for Crisis Management E&T



Orlin Nikolov and Kostadin Lazarov

## 1 Introduction

The history of human beings is nothing more than a history of wars, in which three wars have been fought each year on the average. Millions of people have suffered throughout this history and still are suffering from the consequences of wars, armed conflicts and other disasters. Seventy countries in the world are facing potential or actual armed conflicts in their territory today as a result of conventional and non-conventional threats and risks.

Starting with the 1815 Vienna Congress, followed by the establishment of the League of Nations in 1917, the United Nations in 1945 and other International/Regional Organizations, the International Society has been trying to prevent the wars and the conflicts and to resolve the disputes through an institutionalized system in order to maintain peace and security in the world.

However, the threats and risks we face today are more complex and challenging than ever particularly as a result of globalization. Therefore, we must have efficient mechanisms and we must establish robust procedures to address the security problems to prevent them from developing into crises or conflicts and to relieve and recover the tragic impacts on the people.

Speaking about crisis management we should find in general that it is a huge comprehensive process including almost everything to keep and build resilience on national and alliance levels.

When we speak about who is involved, who are the main actors and what are their responsibilities we will see that the cooperation and collaborations in the area

---

O. Nikolov (✉) · K. Lazarov

Crisis Management and Disaster Response Centre of Excellence (CMDR COE), Sofia, Bulgaria  
e-mail: [orlin.nikolov@cmdrcoe.org](mailto:orlin.nikolov@cmdrcoe.org); [kostadin.lazarov@cmdrcoe.org](mailto:kostadin.lazarov@cmdrcoe.org)

are crucial with a lot of national and international actors, governmental (GO) and non-governmental (NGO) organizations.

When we talk about crisis and disaster management, we should talk about responsibilities and saving human life, financial and material losses. For that reason, the responsible person should have a lot of knowledge and education in multidomain aspects.

Historically, government at all levels, local, state and national has played a large role in crisis management. Indeed, many political philosophers have considered this to be one of the primary roles of government. Emergency services, such as fire and police departments at the local level, and the National Guard at the federal level, often play integral roles in crisis situations.

To help coordinate communication during the response phase of a crisis, different National Response Plans (NRP) on national levels or Crisis Management/Response Plans on multinational level such in UN, NATO, EU should be activated. This plan is intended to integrate public and private response by providing a common language and outlining a chain-of-command when multiple parties are mobilized. It is based on the premise that incidences should be handled at the lowest organizational level possible. The NRP recognizes the private sector as a key partner in domestic incident management, particularly in the area of critical infrastructure protection and restoration.<sup>1</sup>

## 2 Definitions

Defining *crisis* and relatedly—*crisis management*, would be key to simulating planning and decision-making for response.

From an etymological perspective, the word crisis comes from the Greek κρίσις and it means “decision.”

Despite its frequent use, no collectively accepted definition of a crisis exists.

According to the context in which the word crisis is used, different definitions have been given to the concept and the vast majority of them describe crisis as any event that is going (or is expected) to lead to an unstable and dangerous situation affecting an individual, group, community or whole society. Crises are deemed to be negative changes in the security, economic, political or societal environmental especially when they occur suddenly, with no time and warning.<sup>2</sup>

An Ad Hoc Working Group in NATO defined Crisis as *a National or International situation in which there is a threat to priority values, interests or goals*. Although this definition is not an agreed definition it is comprehensive enough that it covers all types of Crises that might have to manage or assist in managing.

<sup>1</sup> For detailed review on definitions see: Heath, 2012; James et al., 2011; Jaques, 2009; Pearson & Clair, 1998; and Sellnow & Seeger, 2013.

<sup>2</sup> Community – Wikipedia.

Despite a diversity of perspectives and intellectual traditions, the analysis has been made<sup>3</sup> of the multiple definitions of crises and crisis management over the past 20 years reveals convergence.<sup>4</sup> Drawing from this convergence, we define an organizational crisis as an event perceived by managers and stakeholders to be highly salient, unexpected and potentially disruptive. We also recognize that crises have four primary characteristics: (a) crises are sources of *uncertainty, disruption and change*;<sup>5</sup> (b) crises are *harmful or threatening* for organizations and their stakeholders, many of whom may have conflicting needs and demands;<sup>6</sup> (c) crises are *behavioural phenomena*, meaning that the literature has recognized that crises are socially constructed by the actors involved rather than a function of the depersonalized factors of an objective environment<sup>7</sup> and (d) crises are parts of larger *processes*, rather than discrete events.<sup>8</sup> Additionally, we recognize that crisis management broadly captures organizational leaders' actions and communication that attempt to reduce the likelihood of a crisis, work to minimize harm from a crisis and endeavour to re-establish order following a crisis.<sup>9</sup>

Definitional convergence aside, a number of scholars prior to and throughout our review period have noted a lack of integration across disciplines and perspectives.<sup>10</sup> For example, Shrivastava highlighted a "Tower of Babel" effect, arguing that there are "many disciplinary voices, talking in so many different languages to different issues and audiences"<sup>11</sup> that it becomes difficult to build cross-disciplinary theory and policy guidelines. More recently, Pearson et al. worried that the "virtual galaxy of critical concepts" resulting from this lack of coordination not only may impede on the ability to build theory and aid practice but also risks the "legitimacy and credibility" of the field as a whole.<sup>12</sup> James et al. echoed this concern in their review of crisis leadership, noting that "fragmentation has prevented a widely accepted understanding of, or commitment to, a common research paradigm in the field of crisis management."<sup>13</sup>

---

<sup>3</sup> Journal of Management Volume: 43 issue: 6, page(s): 1661–1692 Article first published online: December 8, 2016; Issue published: July 1, 2017, Jonathan Bundy, Michael D. Pfarrer, Cole E. Short, W. Timothy Coombs.

<sup>4</sup> see Heath, 2012; James et al., 2011; Jaques, 2009; Pearson & Clair, 1998; and Sellnow & Seeger, 2013, for detailed definitional reviews.

<sup>5</sup> Bundy & Pfarrer, 2015; James et al., 2011; Kahn et al., 2013.

<sup>6</sup> Fediuk, Coombs, & Botero, 2012; James et al., 2011; Kahn et al., 2013.

<sup>7</sup> Coombs, 2010: 478; Gephart, 2007; Lampel et al., 2009.

<sup>8</sup> Jaques, 2009; Pearson & Clair, 1998; Roux-Dufort, 2007.

<sup>9</sup> Bundy & Pfarrer, 2015; Kahn et al., 2013; Pearson & Clair, 1998.

<sup>10</sup> Jaques, 2009.

<sup>11</sup> Shrivastava, 1993, p. 33.

<sup>12</sup> Pearson et al., 2007, p. viii.

<sup>13</sup> James et al., 2011, p. 457.

It can clearly be seen in the definition, Crisis Management is not only managing the conflict, but it also refers to and covers both the prevention and the resolution of Crisis.

Collective defence is at the heart of the Alliance and creates a spirit of solidarity and cohesion among its members. Crisis management remains to be one of the fundamental security tasks for Nations and the Alliances. It commits to be ready, case-by-case and by consensus, continuously to monitor and analyze the international environment, to anticipate crises and, where appropriate, take active steps to prevent them from becoming larger conflicts. In crisis, military and non-military measures can be involved to respond to a threat, both in a national or international situation.

The UN Charter is the framework document within which the Alliance operates. In the Washington Treaty, Allies reaffirm their faith in the UN Charter and commit themselves to the peaceful resolution of conflicts.

In the adoption of NATO Strategic Concept in 2010, the Alliance committed to preventing crises, managing conflicts and stabilizing post-conflict situations, including by working more closely with NATO's international partners, mainly with the UN and the European Union.

The Crisis Management and Disaster Response Centre of Excellence (CMDR COE) defines crisis as “*a time-bound state of (objective or subjective) uncertainty and major non-routine events putting to the test the overall resilience and preparedness of a system and its established procedures and emphasizes on a much underestimated aspect of emergencies—the different experiences of insecurity.*”<sup>14</sup> As Vaklinova notes, resilience “prevents external factors from turning into external stressor factors as a system ‘communicates’ with the external environment and with other systems.”<sup>15</sup>

Walking through this diversity of definitions, it becomes evident that the conceptualization of crisis would reflect organizational mandate, purpose and capabilities, and hence, inform actions.

The CMDR COE defines *crisis management* as “an iterative process of organized and coordinated actions, by and among all responsible stakeholders at the local, national, regional and international levels.”<sup>16</sup> The aim is to tackle a crisis at all its phases (prevention (before), occurrence (during), recovery (after)), which entails specific expertise, skills and techniques for analysis as well as tailored arrangements with a clear vision and exit strategy.

<sup>14</sup> Source: CMDR COE, available at: [https://www.cmdrcoe.org/menu.php?m\\_id=112](https://www.cmdrcoe.org/menu.php?m_id=112)

<sup>15</sup> Vaklinova, 2019, pp. 12–13. <https://www.cmdrcoe.org/download.php?id=1587>

<sup>16</sup> Source: CMDR COE, available at: [https://www.cmdrcoe.org/menu.php?m\\_id=112](https://www.cmdrcoe.org/menu.php?m_id=112)

### 3 Objectives of Crisis Management (CM)

According to the definitions, we can define what are the objectives of CM. In broad terms, these are:

1. To contribute to effective conflict prevention with reducing tensions in order to prevent them from becoming crises
2. To manage effectively crises and to prevent them from becoming conflicts
3. To ensure timely civil and military preparedness adapted to suit different degrees of crisis
4. If the hostilities break out, to control the response, prevent further escalation and persuade any aggressor to cease his attack and withdraw
5. When the hostilities have been stopped or are under control, to re-establish normal order and restore stability

Figure 1 illustrates the development process of a crisis, which mainly consists of an escalation phase, followed at a zenith, by a de-escalation phase. A typical curve begins at a state that we call “Peace” which implies a crisis state in which there is little or no violence and no threat. The curve then moves upwards to “Disagreement” signifying that a threat is recognized by the parties involved in the crisis.

A further progress of the curve to “Confrontation” indicates that actions of increasing violence are being undertaken by one or more parties to the Crisis. The curve could then rise to a zenith signifying an “Armed Conflict.”

Eventually, crisis intensity will drop, implying a state of “Build-Down” in which the violence is lessening, the worst is over and that adversaries are also working

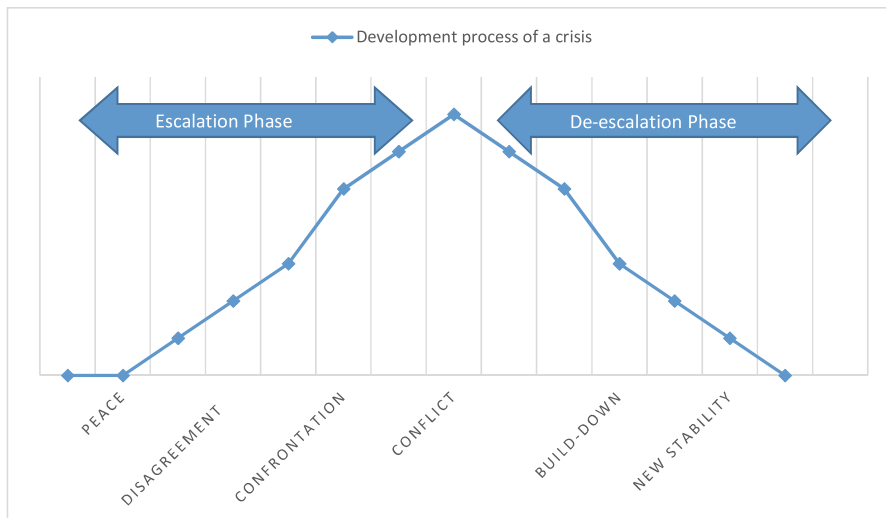
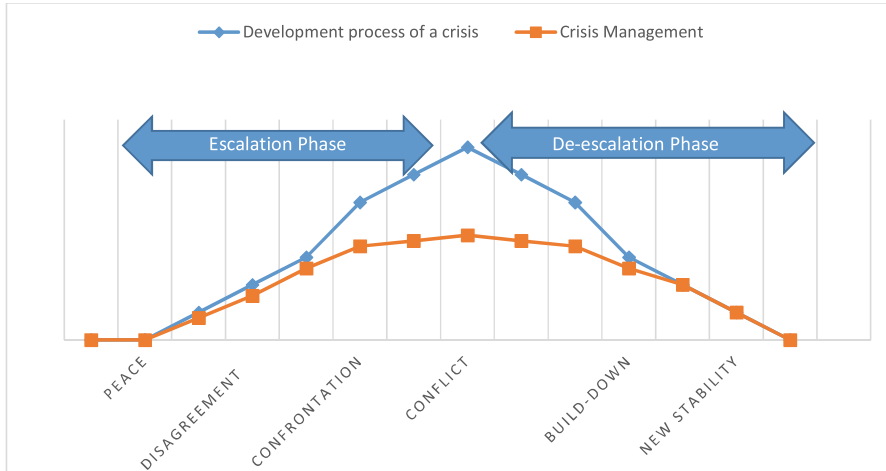


Fig. 1 Development process of a crisis





**Fig. 2** Crisis management

towards a mutually acceptable stable situation. The curve then drops to a relatively low crisis intensity signifying a state of “New Stability” which indicates a new status quo that is acceptable to all parties involved in the Crisis.

As can be seen in Fig. 2, crisis management aims to prevent the rise of the curve upwards by intervening as early as possible into the situation.

The first objective of the Crisis Management efforts is to reduce tensions between the parties to prevent them from developing into a confrontation, and further into an armed conflict. However, if the efforts fail and an armed conflict erupts, Crisis Management aims to contain the intensity of the conflict and persuade the aggressor to cease the attack and withdraw. The final objective of Crisis Management is to achieve a stable and workable situation, acceptable to all parties involved in the crisis.

## 4 Phases of Crisis Management

Usually, there are three major phases in Crisis Management:

1. Preparation
2. Response
3. Resolution

The major activities in the **preparation phase** are:

- Establishment of crisis management structures and bodies, decision-making systems, procedures and relations with respective organizations
- Identification of potential crisis areas and monitoring for the potential crisis areas

- Resource planning
- Training and exercises

The **response phase** starts with a political decision for engaging into the emerging or actual crisis. A response strategy, which later will be translated into a response plan, will be identified when the decision is made. The response strategy can consist of preventive options and/or enforcement options or a combination of both, depending on the situation. The preventive options are peaceful means such as diplomatic and economic means backed by military deterrence whereas enforcement requires the use of military force against the aggressor.

Achieving an agreement between the parties to the crisis is the primary essential activity in the **resolution phase**. The implementation of the agreement and the monitoring of the implementation are two other important major activities in this phase. Disengagement of the crisis establishments and means from the crisis area will take place as the provisions of the agreement are met.

## 5 Trends in Crisis Management

There exist three widely addressed aspects that mark crisis management efforts. *First*, the need for a **comprehensive** all-hazard approach (conventional & non-conventional) to tackle the complexities of the current and future operating environment. *Second*, the demand for a multidisciplinary threat analysis and *third*, wide cooperation to reflect interconnectedness and interdependence of systems, i.e. diplomatic, social, economic, military, psychological, legal, informational and the transnational character of threats. A *fourth* one, we argue, merits increased focus and attention as it bridges theory with practice in a holistic manner. Providing required **Training and education** for decision-makers is essential to raise awareness on and exercise the application of modern software, models and programmes for timely and informed decisions.

## 6 NATO Crisis Management Concept<sup>17,18</sup>

Crisis management remains to be one of the fundamental security tasks for the Alliance. It commits the Alliance to be ready, case-by-case, and by consensus, continuously to monitor and analyze the international environment, to anticipate crises and, where appropriate, take active steps to prevent them from becoming

---

<sup>17</sup> <https://www.nato.int/>

<sup>18</sup> Crisis Management and Disaster Response Centre of Excellence lectures fond.

larger conflicts. That is the reason why we would like to point out in detail how the Alliance as NATO managed the crisis.

NATO can involve military and non-military measures to respond to a threat, be it in a national or international context. Where conflict prevention proves unsuccessful, NATO will be prepared and capable to manage hostilities. As stated in the Alliance's Strategic Concept (2010) "*NATO will [...] engage, where possible and when necessary, to prevent crises, manage crises, stabilize post-conflict situations and support reconstruction.*" This encourages a greater number of actors to participate and coordinate their efforts and considers a broader range of tools to be more effective across the crisis management spectrum. This comprehensive approach to crises, together with a greater emphasis on training and capacity-building for local forces goes hand-in-hand with efforts to enhance civil-military planning and interaction.

The United Nations Security Council has the primary responsibility for the maintenance of international peace and security in the World. However, Article-51 of the UN Charter recognizes the inherent right of individual or collective self-defence of the UN Member Nations.

NATO was founded as a regional collective defence organization in 1949 with the aim of maintaining the security of the North Atlantic Area, on the legal basis of UN Charter Article-51.

1949 Washington Treaty, the Foundation Treaty of NATO, constitutes the basic legal framework for NATO and the NATO Crisis Management. The first seven articles of the Treaty, in particular Article-4, Article-5 and Article-7 establish the legal basis for NATO Crisis Management.

Article-4 is the basis for the consultation process by expressing that the Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened. Article-4 directs the NATO Crisis Management as in two ways; first, any recognized threat by any of the member states could be a case to be considered by the Alliance that may potentially require a response. Secondly, it establishes the method of Alliance decision-making system based on consultation.

NATO's Article-5 states that *an armed attack against one or more of them in Europe or North America shall be considered an attack against them all.*<sup>19</sup> Article-5 outlines the way of individual or collective response to the armed attacks, which has been the focus of NATO Crisis Management during the Cold War and still is the most important component of NATO Crisis Management.

Article-7 states that *This Treaty does not affect, and shall not be interpreted as affecting in any way the rights and obligations under the Charter of the Parties which are members of the United Nations, or the primary responsibility of the Security Council for the maintenance of international peace and security.* NATO accepts and respects the primacy of the United Nations for the maintenance of International Peace and security with Article-7.

---

<sup>19</sup> [https://www.nato.int/cps/en/natohq/official\\_texts\\_17120.htm](https://www.nato.int/cps/en/natohq/official_texts_17120.htm)

The Washington Treaty itself clearly subordinates the Alliance to the UN Charter. In the same vein, the preamble and Article-1 of the Washington Treaty confirm the Alliance adherence to UN primacy.

It is useful to note the agreed objectives of NATO crisis management.<sup>20</sup>

In broad terms, these are:

1. To contribute to effective conflict prevention including contribution for reducing tensions so as to prevent them from becoming crises which could affect the security of Allies and through crisis response options
2. To manage effectively crises which have arisen to prevent them from becoming conflicts
3. To ensure timely civil and military preparedness adapted to suit different degrees of crisis
4. In the very unlikely event that hostilities break out, to control the response, prevent further escalation and persuade any aggressor to cease his attack and withdraw
5. And when further escalation of hostilities have been stopped or are under control, to de-escalate in order to re-establish normal order and restore stability

The NATO crisis management basic principles embedded into NATO CM policies are:

- Supremacy of North Atlantic Council (NAC)—NAC is highest authority of the alliance.
- Consensus—all decisions are made by consensus.
- Permanent representation of NATO nations—they represent all elements of the government.
- Political control over the military—military has the power but politics exercise the authorization. When a crisis occurs, no decisions on planning, deployment or employment of military forces are taken without political authorization.

With regard to NATO's cooperation with international organizations, NATO places a great emphasis on cooperation with the EU, UN and Organization for Security and Co-operation in Europe (OSCE). NATO and its Allies indeed share common objectives and values with the above-mentioned organizations, such as preservation of international peace and security and respect for human rights, freedom, democracy and stability.

NATO's cooperation with the EU is especially important taking into account that the majority of NATO member states are also EU members.<sup>21</sup> While NATO-EU cooperation officially started in 2001, the cooperation gained real momentum in

---

<sup>20</sup> NATO Crisis Management response Manual.

<sup>21</sup> **Out of the 27 EU member states, 21 are also members of NATO.** Another four NATO members are EU applicants—Albania, Montenegro, North Macedonia and Turkey. Two others—Iceland and Norway—have opted to remain outside of the EU, however participate in the EU's single market.

2016 and 2018 by the adoption of the two Joint Declarations, respectively. In these declarations, NATO and EU pledged to strengthen cooperation in the areas such as countering hybrid threats, operational cooperation at sea and on migration, cyber security and defence, defence capabilities, defence industry and research, exercises and supporting Eastern and Southern partners' capacity-building efforts.

Long before NATO had set up cooperation with the EU, NATO already had in place effective cooperation with the UN.

Since the early 1990s, NATO and the UN have been consistently enhancing and developing cooperation. Especially, in the area of operations.

All NATO-led operations in the Western Balkans, Afghanistan and Libya implemented binding UN Security Council Resolutions.

In addition, the NATO training mission in Iraq was set up partly pursuant to a UN Security Council Resolution. In addition to peace support and peacekeeping operations, NATO-UN cooperation covers a wide variety of fields, such as crisis assessment and management, civil-military cooperation, training and education, promotion of the role of women in peace and security, protection of civilians, including children in armed conflict, sexual and gender-based violence, arms control and non-proliferation as well as the fight against terrorism.

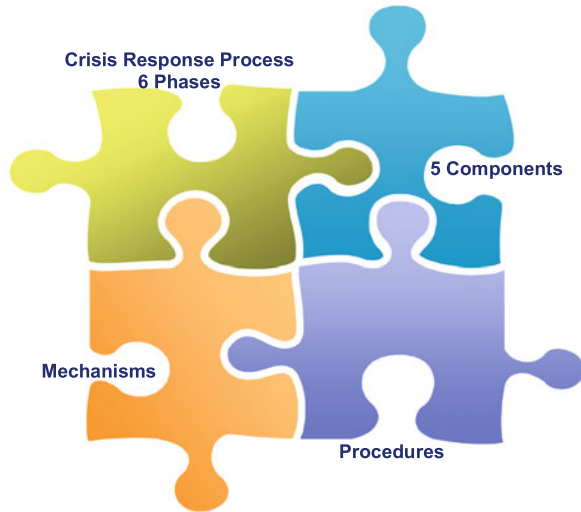
Finally yet importantly, NATO cherishes cooperation with the Organization for Security and Co-operation in Europe. This cooperation includes but is not limited to combating transnational threats, including terrorism and cyber threats, border management and security, disarmament, small arms and light weapons, as well as regional issues and exchange of experience on the respective Mediterranean dimensions.

It is also worth mentioning the Cooperation with Partner Nations. In order to contribute to peace and stability outside the Alliance, throughout the years NATO has established different partnerships with third nations and developed different partnership programmes, such as: Partnership for Peace Programme, Mediterranean Dialogue, Istanbul Cooperation Initiative and the Euro-Atlantic Partnership Council.

At the Wales Summit in September 2014, NATO leaders adopted a comprehensive Partnership Interoperability Initiative to enhance NATO ability to tackle security challenges together with our partners. The sets in place measures designed to ensure the deep connections built up between partner forces over years of operations will be maintained and deepened so that they can contribute to future NATO and NATO-led operations and, where applicable, to the NATO Response Force.

Through Partnership Interoperability Initiative (PII) initiative, an Interoperability Platform format has been set up, bringing together Allies with partners that have demonstrated their commitment to reinforce their interoperability with NATO (22

**Fig. 3** NATO crisis response system



partners so far<sup>22</sup>). Meeting in the Interoperability Platform format, Allies and partners will discuss and develop common actions to deepen their interoperability.

There were also discussions with five partners<sup>23</sup> that make particularly significant contributions to NATO operations to discuss further deepening dialogue and practical cooperation as part of the enhanced opportunities within the Partnership Interoperability Initiative.

NATO stands ready to consider the addition of other partners as their contributions and interests warrant.

Here is the time to mention that CMDR COE as part of the wider framework supporting NATO Command Arrangements, actively provides the necessary expertise to both Member States and the Alliance's partners. For instance, since 2018, the Centre has been part of NATO Defence Capacity-Building Initiative and was involved in the process of improving the structures and procedures of the newly established National Centre for Security and Crisis Management of Jordan.

Let us clarify the term system, and then we will move to NATO Crisis Response System (NCRS). Many authors describe system as an orderly grouping of interdependent components organized for a common purpose.

Similarly, as can be seen in Fig. 3, the NATO Crisis Response System has its elements. It consists of Crisis Response Process, different components, mechanisms and procedures.

<sup>22</sup> Armenia, Australia, Austria, Azerbaijan, Bahrain, Bosnia and Herzegovina, Finland, Georgia, Ireland, Japan, Jordan, Kazakhstan, Republic of Korea, Republic of Moldova, Mongolia, Morocco, New Zealand, Serbia, Sweden, Switzerland, Ukraine and the United Arab Emirates.

<sup>23</sup> Australia, Finland, Georgia, Jordan and Sweden.

The five components of the System are: Preventive options, Crisis Response Measures, Counter Surprise, Counter Aggression and NATO Security Alert States.

For instance, Preventive options are general courses of actions available for consideration by senior NATO committees designed to prevent escalation of a developing crises. These are diplomatic, economic and military options.

The Crisis Response Measures are detailed actions, which are available to be immediately implemented at the appropriate levels. These actions are prepared in advance.

As a vital element of the NATO Crisis Response System, a special attention deserves the NATO Crisis Response Process. It is a six-phase consultation and decision-making process.

1. Indications & Warning
2. Assessment
3. Response Options Development
4. Planning
5. Execution
6. Transition

The process can be adapted easily to any crisis situation and also provides a procedural structure that allows the Supreme Allied Commander Europe to undertake some prudent preparatory planning activities in light of a developing or actual crisis and, subsequently, to provide strategic assessments.

Thus, the NCRS serves as the Alliance's overarching procedural architecture against which both military and non-military crisis response planning processes should be designed.

Lessons learned from NATO operations reveal that addressing crisis situations calls for a comprehensive approach combining political, civilian and military instruments. Building on its unique capabilities and operational experience, NATO can contribute to the efforts of the international community for maintaining peace, security and stability, in full coordination with other actors. Military means, although essential, are not enough on their own to meet the many complex challenges to our security. The effective implementation of a comprehensive approach to crisis situations requires nations, international organizations and non-governmental organizations to contribute in a concerted effort.

The lessons learned from NATO operations, in particular in Afghanistan and the Western Balkans, make it clear that a comprehensive political, civilian and military approach is necessary for effective crisis management. The Alliance will engage actively with other international actors before, during and after crises to encourage collaborative analysis, planning and conduct of activities on the ground, in order to maximize coherence and effectiveness of the overall international effort.

The new security environment poses very complex threats and these threats, risks or concerns usually have global implications as a result of increasing interdependence of world events or relations. Therefore, the challenges that would have to be faced in the new environment could not be comprehensively addressed by one institution alone but only in a framework of international cooperation. NATO plays

an important role by providing the framework for consultation and coordination of policies between NATO and other international organizations and between NATO and Non-NATO countries from the Central Asia, the North Atlantic and the Europe in order to diminish the risk of crises, which could impinge on common security interests.

The best way to manage conflicts is to prevent them from happening. That is the reason staff education and training must be a continuous process every day.

## 7 Needs of Joint Actions

The need to establish national, regional and allied initiatives for the cohesion of forces supporting the training and preparation of structures designated for participation in both purely military missions and non-military missions should support the educational process conducted by educational institutions (academies, universities, colleges, schools) and create an integrated resource library that stores a rich collection of data related to the conduct of exercises, seminars and other forums in the field of modelling and simulations and Computer-Assisted Exercises. The challenges of natural disasters, as well as the consequences of climate change during EU operations, underline the need for sound strategic, operational, organizational and logistical planning. Given the potentially diffuse nature of a crisis, as well as the associated time-critical nature of decision-making processes, the requirement for a comprehensive approach is necessary in the use of data, standardization of information collection processes, modelling and simulation and ultimately accounts for the preparation for disaster risk analysis and management. The improvement of the aspects of training and preparation of the National Crisis Management Systems is conditioned by the need to ensure the necessary training of the country's leadership, the population and the national economy for protection in case of crises, preservation and optimization of the existing elements of the crisis management system, development of bodies and mechanisms for action in the integrated management system and ensuring compatibility with the crisis management mechanisms in NATO and the EU.

The ability to respond to crisis management and disaster response inquiries will be rich with operational experience to provide subjective responses and training activities. However, this gap will require a pre-feasibility and scoping study to determine if it is eligible for support using modelling and simulation (M&S).

However, the capabilities of the CMDR Training and Climate Changes preparedness can be greatly enhanced and increased with the addition of some unique crisis management and disaster response tools, software and simulation systems.

The additional creation of an M&S Laboratory specialized for CMDR Training and Climate Change preparedness would provide NATO with a unique comprehensive training and analytical capability unmatched anywhere in the world and enable non-military type operations. This M&S Laboratory would be able to support large-scale CMDR-distributed exercises and analyses with specific crisis management



and disaster response tools and simulations. There should also be experienced and highly trained personnel to operate this newly established Laboratory. This new crisis management and disaster response Laboratory should also be supported by operationally experienced simulation experts to ensure successful operations, exercises and support activities right from the beginning of operation.

By more effectively integrating this aspect, the NATO force structure can be more prepared for the next conflict by support in capability-building; improving interoperability and support of capability development with education and training for NATO and partner leaders and units; testing doctrines; developing and validating concepts through experimentation; providing lessons learned, evaluations and assessments.

All this determines the imposed need to create a technical architecture and disaster modelling module that will allow each decision to be reproduced and visualized to the decision-maker and to assess in real time what damage the disaster will cause to personnel, infrastructure and equipment. This makes it possible to assess the material damage and play different options for action by choosing the most optimal response plan. Also, after the actual completion of the operation, an analysis of the current procedures can be made, adjusted and improved accordingly.

The objects of the technical architecture are the applied procedures, material, communication, information base and the bodies that provide and use them, as well as the forces and resources that form a mechanism for crisis resolution. The effectiveness of the mechanism depends on the organization to conduct an immediate and continuous process of coordination between the competent state agencies and bodies, as well as with NATO, the EU, the UN and its agencies, the OSCE and individual countries. The study of the national training systems, as well as the NATO and EU training systems, provides an answer to the question of what needs to be improved in the training of all personnel responsible for inter-institutional coordination, through which they can solve crisis management problems and disaster response.

As we have already seen, the crisis and disaster management process is a complex process with many components that cannot be covered by one organization. Therefore, the technical architecture provides an opportunity to achieve higher management efficiency through the training of personnel for crisis management and more precisely the use of models, simulation systems and conducting computer-assisted exercises as a form of preparation, experimentation, testing and validation of new regulations and its implementation in crisis management systems.

Creating a collaborative, global network of crisis management preparedness capabilities using the full range of live, virtual and constructive simulations and disaster prediction models is vital to helping in order to increase the effectiveness of the crisis management process. The transformation of the training system by building joint training capabilities at National and Allied levels is used to significantly improve joint training, exercises and training with participants from different ministries and departments and to attract governmental and non-governmental organizations. It helps to complete training programmes and supports the planning of new extended joint exercises to increase interoperability in a common distributed training environment.

Improving the effectiveness of education and training systems at national and Allied levels can only be achieved by offering a wide range of civil-military instruments, interaction and coordination between institutions and with partners, applying a comprehensive approach not only nationally but also mostly at the international level by creating a unified environment for improving expertise.

## 8 Building Resilience

As to the element of awareness, NATO is concentrated on gaining appropriate military capabilities<sup>24</sup> at the expense of other instruments of power which are not developed in the field of economy and diplomacy. In order to have other instruments of power at its disposal, which are crucial for combating hybrid threats, NATO has to establish relations and a level of coherence with other actors such as the EU. In order to counter hybrid threats, security should be perceived as a broad concept, because these threats endanger the integral security of the whole society. Therefore, in countering it, all relevant actors should be engaged, thereby enhancing the process of transformation of NATO (including COEs). This will lead to a stronger political position, a clear strategic direction and availability.

Resilience is an essential basis for credible deterrence and effective fulfilment of the Alliance's core tasks. Under the North Atlantic Treaty (particularly Article-3),<sup>25</sup> all Allies are committed to building resilience. In today's security environment, resilience more than ever requires a full range of capabilities, military and civilian and active cooperation across governments, and with the private sector. It also requires engagement with partners and other international bodies, and continuously updated situational awareness.

Hybrid threats inevitably encompass a combination of full range of different modes including conventional capabilities, irregular tactics and formations, terrorist acts, including indiscriminate violence and coercion against civilians and criminal disorder, which endangers the civilian population. In such a [dis]order, hybridized actors have the means to surprise and spread fear throughout the traditional nation-state community. These threats display different sorts of tactics, typical for asymmetric warfare and in particular for terrorism such as armed assaults against civilians, bombings (including suicide bombing) and explosions (including improvised explosive devices), assassinations, hostage taking of civilians such as kidnapping and hijacking. The violence included in hybrid threats is directed against the civilian population.<sup>26</sup> That is so because terrorism is a political tactic, which

<sup>24</sup> "Readiness Action Plan," *NATO Topics*, last updated September 21, 2017, accessed April 5, 2018, [http://www.nato.int/cps/en/natohq/topics\\_119353.htm](http://www.nato.int/cps/en/natohq/topics_119353.htm)

<sup>25</sup> In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack.

necessitates the utilization of violence or the threat of violence against civilians. The use of violence against civilians is rational, premeditated and has as a purpose the achievement of the ultimate objective, which should be political. The motives can be different. The threat of using violence or the real use of violence is precise in terms of terrorist strategy and indiscriminate in terms of victims. Terrorists intend to produce extreme fear or terror and to exploit insecurity created by the fact that the population is put in fear.

Therefore, and for the purpose of building resilient society, the main priority of the international community and its main efforts should be directed against hybrid threats, and in particular terrorism which exploits the vulnerability of the democratic societies and seeks to spread, fear. The concentration on protection of civilians in times of hybrid threats is a must and a core for the field of security.<sup>27</sup>

The word resilience is not quite new and this fact proves that this is not an up-to-date idea but a phenomenon ancient as human society. More interesting is the question how we can measure resilience on national or societal principles. That is a very tough task, which should include a lot of known and unknown parameters where every one of them could play a crucial role in different situations.

More important first look conclusion which we make is that the more developed and democratic a society is, the more resilient it is to various concussions, emerging disasters or crises.

That is one part of the research which CMDR COE started and included in the development of the technical architecture, described below.

Every complex system as human society has parameters describing its static properties and dynamic behaviour.

One of the most important is the property to keep the desired state—position, direction and velocity (positioned vector)—of the system at specific conditions under external influence—resilience.

Resilience is a common property for many objects and has different realizations. Society resilience means that the society will generate a counterforce when an impact over its moral and ethical values (starting point, speed of change and direction) is detected.

Society resilience is observed when the individuals accept low to severe personal discomfort in the name of the society, because it is recognized as more valuable.

The resilience tries to keep the vector when it is threatened but at the same time it has a negative impact over it when such influence is missing.

As can be seen in Fig. 4, the resilience has two components: basic—family resilience; and organized—maintained by authorities. Both of them consume manpower, resources and energy.

Naturally their relationship is inversely proportional. When the basic resilience is high, it is not necessary for the local authorities to maintain high-organized resilience. Vice versa when the organized resilience is high, the basic resilience

---

<sup>26</sup> Orlin Nikolov, *Information and Security: An international Journal*, v.39:1, 2018, 91–110.

<sup>27</sup> Orlin Nikolov, *Information and Security: An international Journal*, v.39:1, 2018, 91–110.

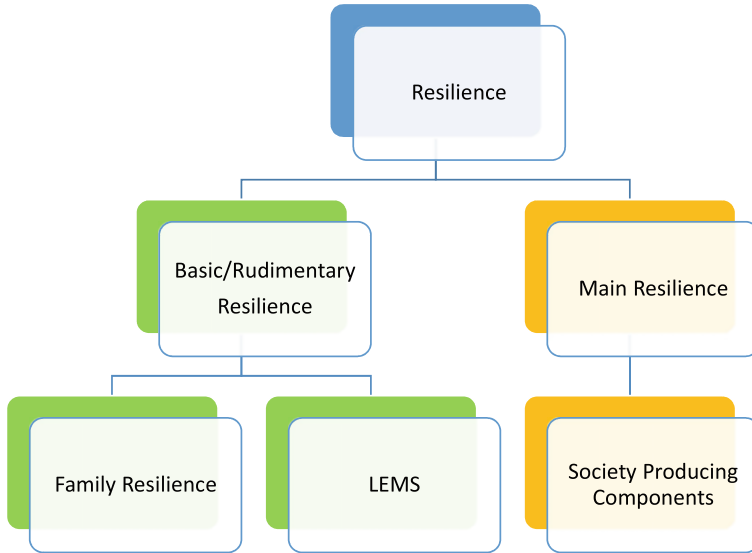


Fig. 4 Resilience structure

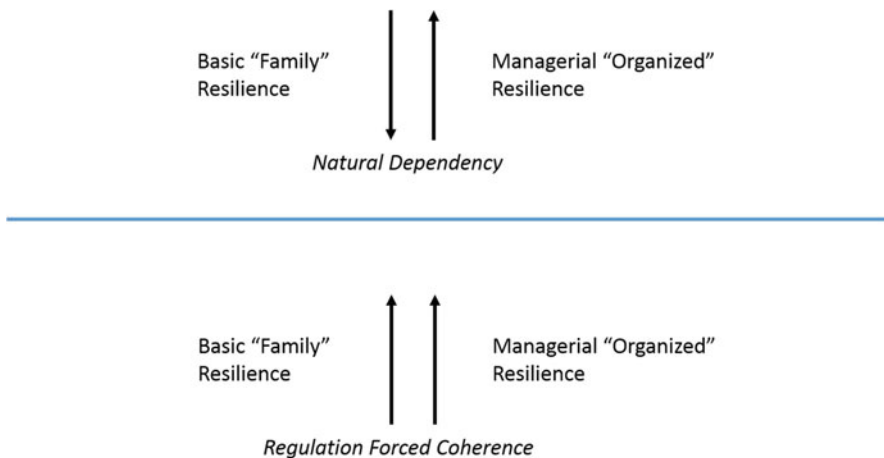
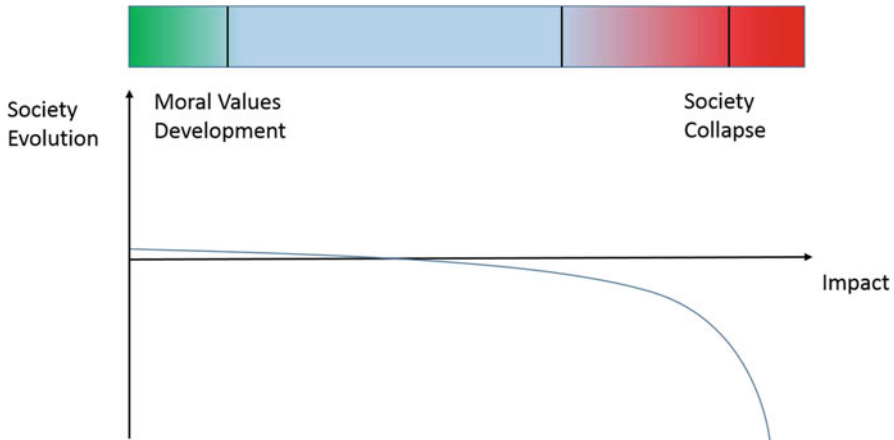


Fig. 5 Resilience dependency

is going down (Fig. 5). One way to fix the problem is the regulations. The organized resilience should rely partially on the basics and should define the interaction between them—coherent synergy. This is also valid for other structures and organizations like NATO. The frequent and adequate update of the regulations and advice to each member concerning their own defence systems, how they should contribute and react, could not only increase the effectiveness and efficiency, but also to draw together the national society vectors.



**Fig. 6** Impact and the function of the society development

It is difficult to calculate the efficiency of the combined resilience. It is integral of what is spent and the difference of the status of the described vector with and without reaction.

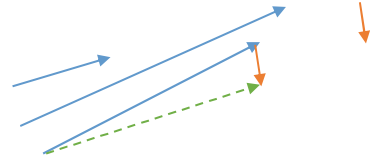
The problem is that an effective way to increase and keep the resilience at a high level is to spend more and more money which could fund culture and science for example. The resilience system consumes more than it adds to society when a thread is missing. The positive part is mostly development of management theory and knowledge.

On the Fig. 6 are shown the impact and the function of the society development. The natural small values of external impacts (noise) have a positive effect over the trend. It stimulates flexibility and creativity. A degradation is observed after specific for each society threshold. The particular value is a function and depends on a few but complex parameters. The moral and ethical values could erode in order to sustain the society. The process is reversible at specific points. Further the society is so deeply affected that it collapses and starts the survival of individuals. Society is lost and cannot be exactly reproduced.

The society as opposed to the forming of its individuals is objective. It has properties as mass and energy and they defined the critical thresholds mentioned above. The external impact most of the time is also vector dependable of the time and space but less dimensional. High value and short impact causes change of the society development velocity. Low value and long impact could change the direction. When a system of subsystems is observed—like international organization—such deviation in the vectors direction reduces significantly the effectiveness and progress speed (Fig. 7).

- The vector represents the hybrid impact generated by third country. It is small as value, close to the daily noise but with permanent direction. Applied to only

**Fig. 7** Impact and the change of the society direction



one of the vectors, it will change the direction and could cause deviation in the common position (Fig. 7).

Society inertness is proportional to few parameters and one of them is the number of the population. A nation could have high inertness because of that. A straightforwardly opposing impact vector applied to the society one is not only easily detected but also has to have proportional scale in order to affect. More dangerous are the impacts with direction perpendicular to the society vector. They do not immediately affect the scale of the vector but could change the direction. Such impact mostly generated by intelligent external actors could be placed as value close to the natural noise. The natural noise changes fast and randomly the direction, the artificial one does not. A filter sensing such directed influence could be created.

Modelling of the resilience could be done using statistical/historical data. Starting with some simplification the generated counter force  $F$ , of the society resilience is equal to:

$$F = k \cdot C \tag{1}$$

Where the  $k$  is the assessment of the situation and understanding of how it could influence the society. The  $k$  value varies between 0 and 1, where 0 means that the basic resilience is enough to face the problem and 1 means that the existence of the society is highly threatened. The  $k$  value fixing is subjective process and the subjectivism increases with the management level. Of great importance is the willingness and motivation of individuals in society to endure adversity and discomfort in the name of a better future. The  $C$  are the potential capabilities. Part of them could be generated during the decision-making process (when the situation is unique). They depend on the available staff, regulations (SOPs), resources, technology and location.

So, when the affected society is wealthier it could face impact with bigger value. It is valid especially when not only the society response system has transformable capabilities—flexible, fast and trained core—but also the existing capabilities or new ones could be augmented/generated using the components of the society’s industrial capabilities (Fig. 8).

Conventional approach when the speed and accuracy of the data exchange, decision-making and delivery of the capabilities at necessary points is crucial. It is a catchy response. There are other approaches also. One of them is to monitor and analyze the changes of the environment in order to analyze the risks and threats.

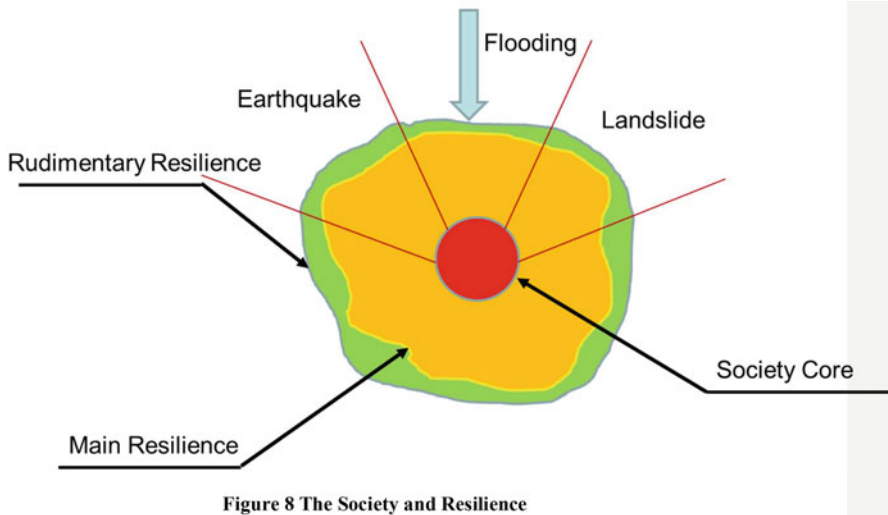


Figure 8 The Society and Resilience

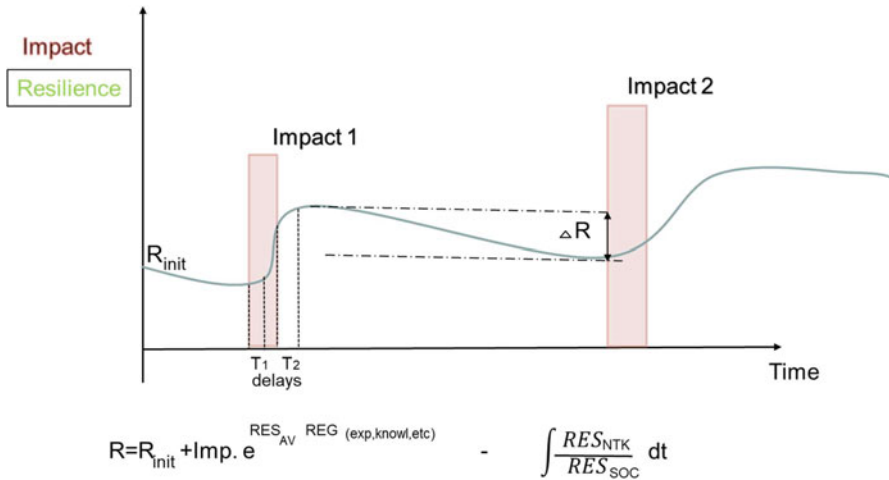
Fig. 8 The society and resilience

The Society core on the graph is surrounded by the main and the rudimentary resilience. The rudimentary resilience is flexible and could absorb the energy of the external negative impact. As it was mentioned, this layer consists of the family resilience and the Local Emergency Management System (LEMS). The family resilience is funded by the individuals of the society and depends on the culture, knowledge, education and regulations to the least extent. Vice versa, the LEMS depends mostly on the regulations. Both components of the rudimentary resilience could generate a defending counter reaction almost immediately. This reaction is limited due to the fact that the basic resilience consumes almost 75% of the resilience expenses. At same time, it generates no more than 25% of the overall resilience. The reason to observe such unbalance is the time for reaction.

The main resilience is generated by the society's main productive forces. Most of the time, even during crisis and disaster events, these forces are engaged in the society production cycle.

In Fig. 9, a possible evaluation of the society's resilience capabilities as a function of impact and time is presented. The function is close approximation of neural network Artificial Intelligence with classical differential equations. The exact problem and proposal for solvation will be reported as a continuation of this article.

The Society Resilience starts from the relative time zero on the graph with initial value  $R_{init}$ . It is slowly decreasing with the time due to the absence of external negative impact.

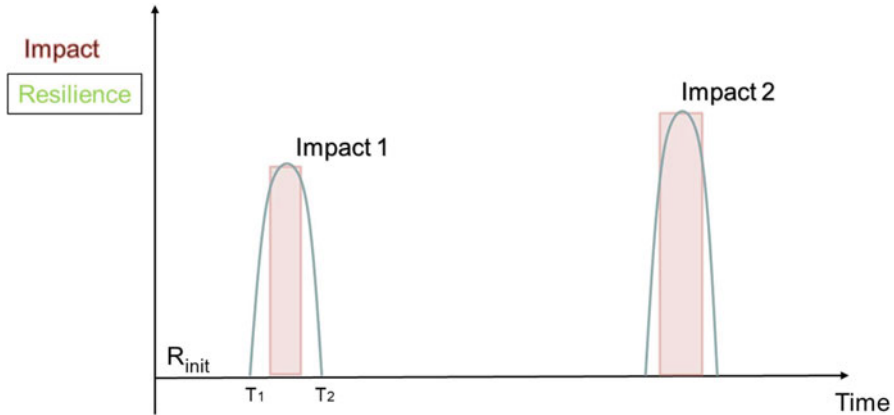


**Fig. 9** Evaluation of the society resilience

The impact is elaborated as a sudden strike with specific value and immediate relief after that. Such an impact could be caused by an earthquake for example. The reaction of the society and the change in the resilience are not instantaneous. Due to some society characteristics, specific delays in the change of the resilience are observed. After the strike of the disaster, the resilience still continues to drop because of the affected society systems and production cycle, information flow and mobility characteristics. Later, the resilience starts to increase its level in order to adequately face the disaster impact and to protect the society’s wealth and means. This increase is related with the escalation of the expenses and a new balance between the basic resilience maintenance cost and capabilities is found. The change of the resilience level does not stop. It will continue to grow after the disaster. The existence of the society in a competitive environment forces it to spend resources in self-development. This is one of the reasons to see gradual decrease of the society’s resilience in absence of negative impact. The resilience cost-level balance is dynamic. If the same disaster strikes again, as it is depicted on the graph, the cycle will start again. The resilience-time function looks almost flat for specific societies and impacts. This is valid for example for Japan where the resilience to such disasters is very high and almost unchangeable due to the frequent occurrence of the event.

Figure 10 shows the Resilience on Demand. In this case, the necessary capabilities are generated at a certain time and location in order to face the specific negative impact. The times T1 and T2 in this case are the periods necessary to generate the capabilities and to release them after the crisis situation. In such a manner, all the resilience level maintenance expenses are saved. The problem is that there is not available information for the nature, time and location of the upcoming crisis and disasters. Even with such preliminary information, it will still be necessary to





**Fig. 10** Resilience on demand

maintain a certain initial Resilience and it is related with the knowledge, theory and concept of crisis and disaster management. Analyzing the first graph, it is also valid—the resilience expenses are significantly reduced with the improvement of the crisis management.

## 9 CMDR COE Technical Architecture

Because of the reasons above, CMDR COE started a project<sup>28</sup> of building a specific framework to support study and research in crisis management, to test and validate concepts and doctrines, to analyze the physical impact and human behaviour.

The importance of the disaster events, their influence and severe impact over human life is indisputable and largely taken under consideration. The planning process and performance of the NATO military operations do not exclude disaster management also.

The significant unpredictability, concerning the time and space occurrence, and the event parameters, make the risk management and disaster management difficult and resource-consuming process. The evaluation of the dynamic impact over planned and performed military operation is almost impossible without usage of appropriate modelling and simulation tools and software. Such applications are military-oriented software allowing realistic war gaming based on the implemented military units' model database and behaviour.

<sup>28</sup> CMDR COE led a research under NATO STO and formed NATO MSG –147 “Modelling and Simulation Support for Crisis and Disaster Management Processes and Climate Change Implications” 2016–2020.

The project has three main directions for analyzing CDMP in NATO in order to improve E&T and support the decision-making process in the Alliance.

The first pillar is the analysis of Disaster Risk Management (DRM) processes, preceding the development of the Operations Plan. This includes:

- Fast and accurate Disaster Risk Analysis
- Comprehensive approach and correlation assessment among hazards
- Prevention and Preparedness Measures proposals

The second pillar concentrates on Disaster Response during NATO operations by assessing:

- Fast and accurate Disaster Assessment (DA)
- Dynamically generated proposal for Response Plan
- LL process

The third pillar focuses on the development of a module for realistic modelling and presentation of different types of disasters for the purpose of education and training, experimentations, tests and validations.

The technical architecture includes a database, holding data from mathematical models for different disaster types which is visualized in an interface (Fig. 11). The collected results are compared with statistical and historical data from events that have already occurred. Depending on constant indexes such as infrastructure, Geographic Information Systems, vegetation and others, a probability in percent for exactness of the model is shown. In that way, the architecture defines the accuracy of different models for different disasters and every decision-maker could prefer what kind of model to choose to work for different situations.

A disaster risk management assessment is made depending on any given task, whereas during the operation planning phase statistical data or through the operation phase real-time field data are used. Firstly, the architecture was tested through training and exercises and now it is ready to be implemented on an operational (strategic) level. The repository with disaster models is connected through High-Level Architecture (HLA) with federated simulation systems and tools proved there usable for different disasters or crises. The calculated results of the models are published in the simulations as objects. For that purpose, a Federated Object Model (FOM) for different disasters should be created. According to the AMSP-04,<sup>29</sup> a Federation is a union of essentially independent applications (Federates) interoperating using common infrastructure services accessed through well-defined standard interfaces and governed by common agreements on modelling responsibilities, the commonly used Data models and information exchange. A High-Level Architecture (HLA) Evolved Federation is a federation using the HLA standard (IEEE 1516–2010) to specify available infrastructure services and APIs for accessing them. The HLA standard also specifies how to document information exchange using a FOM.

---

<sup>29</sup> AMSP-04 NATO Education and Training Network Federation Architecture and FOM Design.

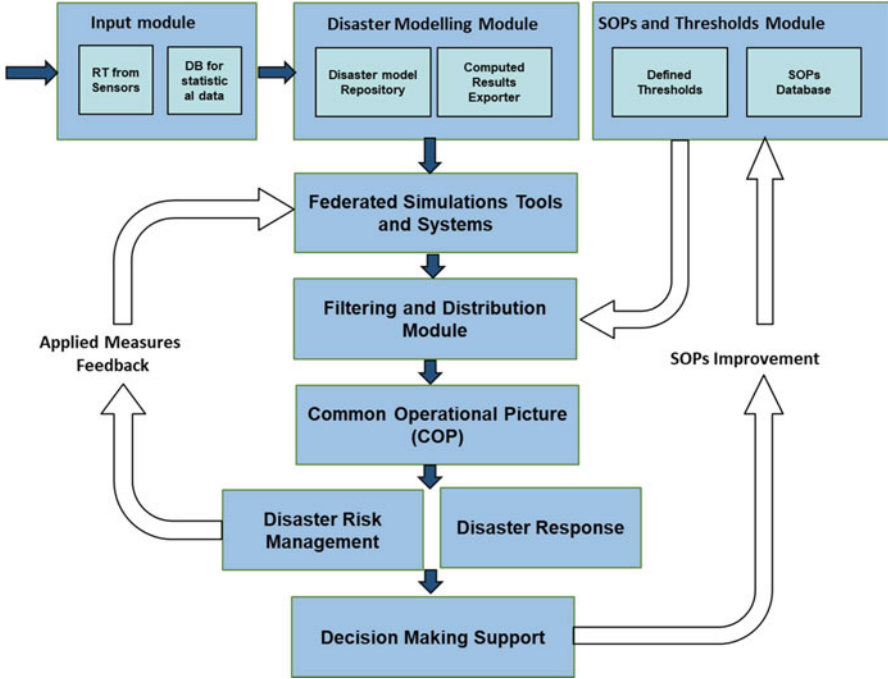


Fig. 11 Technical architecture for CDMP and CCI

During the first phase of the research, it was recognized that there is no existing military-oriented simulation, capable of accurately modelling and simulating all disaster types. Something more, it was realized that the few models (flooding for example) built in are inaccurate and with deviation from one to another simulation.

It makes impossible simulation federation creation, war gaming and following analyses concerning disaster events during military operation.

In order to improve the decision-making process and to increase the objectivism, a Disaster Module application was designed and developed. It is a software with unique capabilities. It could compute and model different disaster events using own or external mathematical models and later could publish the achieved results as standard for the simulation object with all predefined characteristics and attributes. These attributes defining the disaster simulation object are updated frequently. In such a manner, the Disaster Module could distribute one (or more) disaster object to many simulations connected to federation using standard HLA interface. The mathematical model computing the event is outside of the simulations and their responsibility is to estimate the impact over military units, civil society and infrastructure. The Disaster Module provides the software engine for calculations and the necessary operator interface to tune and change parameters. Such approach has many advantages:

- The publish of the disaster as an object into federation of different federates is synchronized and its subsequent updates also.
- The object is same for every federate subscribed for it and does not depend on specific simulation.
- It is not necessary the federate to have own model for the specific event/object/disaster.
- Every disaster mathematical model implemented into Disaster Module is open, very precise and easily changeable if it necessary without changes in the source code of every federate.
- Operator could change the parameters or input data of the mathematical equations describing the disaster mathematical model or to change one model with another if it is more suitable.
- The Disaster Module could publish the computed HLA object representing the desired disaster from its own engine and respective model or using data from another source (like it was experimented with HPAC (with artificial initial conditions and scenario) provided by JCBRND COE. In this case, the Disaster Module serves as a bridge for modelling software and applications not having HLA interface. During the experiments, all technical problems concerning this functionality were solved and finally the data were published and updated as it should.

Later on, to the Disaster Module were attached other modules with different functionalities. Such functionality was the mentioned bridge service allowing transfer of data from not HLA compliant applications to federation. Later on, it was recognized the necessity of services capable of injecting information in the Command-and-Control System, to generate Situational Awareness Report, to propose Response Measures and to visualize them again in C2 environment. Something more, a development of SOP Database started and the first disassembled to rudimentary measures SOPs were provided by SEEBRIG for tests and training support during exercise Balkan Bridges 19.

## 10 CMDR COE Integrated Development Environment

It changed the focus of the application. A decision to make different modules representing the conceptual schema was taken and the name of the software was transformed to Crisis Management and Disaster Response Integrated Development Environment. It elaborates much better not only on the current implemented capabilities and functionalities, but also describes the concept of the product. It is necessary to emphasize again the strictly followed standard interface approach of the development reference architecture. It allows connecting different software and applications with different functionalities and capabilities. Thus, increase significantly the chance for cohesion coordination or synergy.

The CMDR Integrated Development Environment (IDE) has two main roles.

The first one is to connect useful and relevant existing applications like military simulations for example.

In such manner, CMDR IDE configures the necessary framework capable of running war gaming, to publish into the network disaster events of different types, to collect reports about the impact, behaviour and development of the crisis, to run the information through Command-and-Control systems, etc.

This is done by raising interconnections to the clients of the framework. Because of the project's big scale, it was confirmed that the time-saving approach is to use what is currently available like simulation systems, command-and-control systems and networks for information exchange. It was realized that it not only significantly improved the development velocity, but also gave highly advantageous flexibility. Nowadays the CMDR IDE could connect many clients and could transform the final schema easily. Such open architecture allows the interoperability with different applications which is proportional to the potential synergy. It could be elaborated as a function of the common domain of interest and different capabilities.

In the beginning of the project, the schema of the reference architecture covers the cycle of Crisis and Disaster Management. CMDR IDE provides necessary components to build it. Attaching different tools and software to the framework, the architecture could be fully or partially activated. For example, the war-gaming process could start without usage of the module for dynamic plan generation.

This part of the CMDR IDE has a module for transfer of modelled data (computed disaster as an object with specific parameters) to the reference architecture.

This interface is capable of transforming data into simulation compatible from different sources. It is possible because the module can receive the data in various formats. Most of the time the synchronization depends on operator manipulation which actually is advantageous and makes the module more flexible.

Another interface is the simulation-C2 system gateway. It could transfer information from the simulation system to the C2 and vice versa. It is HLA-REST API-based and connects many simulations and C2 systems making large numbers of possible combinations.

The second role of CMDR IDE is related to the innovative part of the project. It was necessary to build a few new applications as additional modules in order to raise the invented architecture.

The first one is the Disaster Module consisting of several submodules: engine running open-source disaster mathematical models, operator interface and almanac database. The operator interface allows one to control some of the coefficients of the mathematical models, to set up the initial parameters (like weather conditions for example). The simulation network gateway is no more part of the module and now is part of the Interface Module.

Module for Information feeding. This module publishes information into the Command-and-Control System. It is used for transfer data from people on the ground in case of disaster or from EXCON if the reference architecture is used for training. It has a simple interface which at the moment is based on Common Alerting Protocol. During the experiments, the module had a simple interface and functionality. Now, under development, is the next version of the module. In it,

**Table 1** Disaster module modelling big-scale events with negative impact over society

Disaster	Own model	External model	Interfaces	Protocols
Flooding	Yes	Yes	REST API, CSV, XML, HLA	Internal, international
Chemical	Yes	Yes	REST API, XML, HLA	Internal, external
Wildfire	No	Yes	REST API, XML, HLA	External
Earthquake	No	Yes	REST API, XML, HLA	External

the EXCON could have a list of preplanned injects making the duties easier and replicable. It saves time and effort.

The CMDR IDE has a main operator interface allowing the user to choose what module related to the Crisis/Disaster Management cycle to start. The CMDR IDE configures the necessary framework disaster mathematical model input data modification or automatic feeding from the sensor network.

The process of feeding the reference architecture with real live/time data is also under development, but some work is done in that direction. CMDR COE has agreement with organizations sources of such information. Initial information about the standards and test sets of data were exchanged. The CMDR COE’s OpsLab also plans to develop hardware capable to monitor objects or subjects and to transfer the data remotely to the technical reference input gateway. It could be used for training, but the main purpose and usage will be for the operational activities.

As it was explained, the Disaster Module could run its own engine with implemented disaster mathematical models (Table 1) or to serve as a bridge between modelling applications without HLA interface and military simulation federation. The advantages of using internal models are knowing of the disaster model mathematical logic and coefficients, its accuracy and the opportunity to modify it when it is necessary. At specific conditions, one mathematical model could be preferred to another. It gives flexibility to the decision-makers. The Disaster Module has a database with reference data for the specific parameters, also. As an example, could be pointed to the value of the gravity acceleration, or the physical parameters of specific toxic gas. The necessary input data depends on the disaster mathematical model requirements. It could be statistical/historical or real-time data. Statistical data are used during Risk Management Analyses (before operation, during the planning process) and real-time during the actual performance of the military operation.

Database Module. The Database Module contains a variety of information. There is stored the almanac data related with specific disasters and necessary for the mathematical models. As an example, could be pointed saturation point of specific soil when the modelled event is flooding.

Another set of tables contain statistical data for the previous disasters. They can be used for analysis, experiments, training, etc. The reason to use such statistical data is realism and objectivism—two trends hardly coded into the project concept. This data, however, could be modified. For example, the location could be shifted

according to the scenario requirements. It gives flexibility and full control in order to conduct beneficial training or experiment processes.

Important part of the Database schema is related with the Standard Operating Procedures (SOPs). The database contains defragmented SOPs with rudimentary response measures at specific levels—tactical, operational and strategic. To each response measure are added metadata which make possible the selective usage of it. Such an approach is innovative since there is no existing similar solution. However, additional formalization of the Disaster Management knowledge, experience and theory should be done.

The Database Module contains also Target List, which is used for the generation of the Dynamic Response Plan. Last but not least here are stored service data related with the transfer of information from simulations to C2 systems and vice versa, preliminary written lists of injections and orders, etc.

## 11 Artificial Intelligence (AI) Module

The purpose of this module is to generate a Dynamic Response Plan. This plan is relevant and adequate to the specific parameters and conditions. It is generated according to the implemented management logic. At the moment of composing this edition, the AI Module is in the initial stage of development. Some tests were performed using a basic schema of thresholds-comparators-triggers. The mentioned target list in the Database Module and the rudimentary response measures are feeding data for the process.

The proposed measures, combined as a raw plan for disaster response, are depicted on the C2 screen making possible its implementation or rejection.

The next step is development of smart AI collecting modern management theory, expertise and knowledge about disaster events and generation of necessary capabilities for response in case of resource shortage.

The desired goal is the AI Module to be capable of selecting the best CoA according to predefined criteria.

The decision-making process at the strategic level is always related to limitations of resources, time and/or manpower. It is naturally encoded in the crisis definition. This fact defines the choice from the available AI algorithms and frames. At the moment for the upper-level decision-making, a game AI algorithm should be used. It is related to the impossibility to prevent losses during a crisis situation or disaster. The game AI is trying to find the best COA despite the minor losses during the management process.

The synergy effect is proportional to:

$$\text{Synergy} = |\text{UntNCpblts} - \text{UntKCpblts}| * \text{NKIntrfc} * \text{ManagementLogic} \quad (2)$$

It is assumed that the synergy effect is proportional to the deviation of the system unit capabilities. The absence of such deviation— $|\text{Unt}_N\text{Cpblts} - \text{Unt}_K\text{Cpblts}|$ —

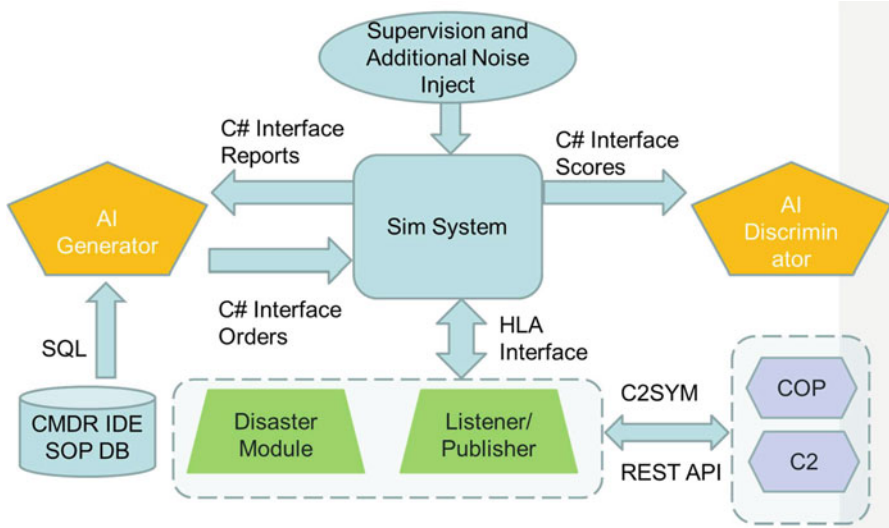


Fig. 12 Planned architecture

excludes synergy existence. On the other hand, there should be a specific interface available for sort of communication between the units. It is not limited to exchange of information. It is represented as one coefficient in the equation in order to simplify it. Finally, the management logic (ManagementLogic) is also proportional to the value of the synergy effect.

In order to seek innovative results from the AI, two independent approaches are planned—usage of GAN AI (Generative Adversarial Network) and unsupervised learning algorithms. Both of them are feeding the game AI at a strategic level.

The GAN AI is powering all tactical and operational units. The unsupervised learning algorithm feeds the game AI directly. In such a manner, the number of the possible management scenarios are significantly limited. This is necessary because of the big number of input parameters for the system.

The planned method includes an increase of the noise injection in the generation of management logic at tactical and operational level. It loosens the constraints on the one hand and reduces the possibility of overtraining the algorithm.

On the schema (Fig. 12) is depicted part of the planned architecture. Here is shown the GAN AI which uses the CMDR IDE as an environment between the two AIs. The environment consists of simulation systems, models of different events (like disaster for example), some restrictive data and rules. The limits are encoded in the SOP Database and the physical models of the simulation system.

Additional adjustment of the cycle is planned with supervision and injection of additional noise directly into the simulation system.

The planned schema is applicable for all represented units at tactical and operational levels. The results of each iteration are used by the unsupervised training algorithm and the results of it go to the game AI at top of the schema.



The architecture consists of almost all CMDR IDE components deployed on three workstations. The HPC workstation runs the AI components. It contains two NVIDIA A100 modules.

## 12 Conclusion

The decision-making support is the way to raise the crisis management quality and speed, to make it effective and efficient. There is a limited number of ways in which the decision-makers could be supported. Modelling and simulations are specific examples. Another approach is collecting and combining knowledge and experience/models in order to immediately propose low-level solutions or to limit the high-level solutions spectrum. It significantly reduces the necessity of available experts on time when a rapid reaction is needed. The AI technology at the moment is satisfactorily applicable despite its own disadvantages. In CMDR COE's OpsLab has started a research of AI technology embedment in the decision-making process.

The research is focused on identification of the crucial components, algorithms and procedures of crisis management. It tries to train an algorithm to find synergetic combinations and coordination in a limited list of units and activities/services.

Training effective and efficient game AI is useful due to some reasons. It could be used in Crisis Management HQs. It could be analyzed in order to find management patterns. Such patterns could be used to improve the management schema and procedures.

## References

1. Multinational Initiatives and Training in Support of Regional Defense Cooperation – BG Marin Nachev, LTC Orlin Nikolov
2. Technical report NMSG 068 “NATO Education and Training Network”
3. Technical report NMSG 147 “Modelling and Simulation Support for Crisis and Disaster Management Processes and Climate Change Implications”
4. ACT Directive for Operating JWC, JFTC and JALLC (80–3), Version: Latest, March 2004
5. ACT Directive for the Implementation of JWC, JFTC and JALLC Plan of Action and Milestones (80-6), Version: Latest, December 2004
6. Provide Joint Training, Experimentation and Interoperability Development Capabilities (CP 9B0401), Version: Latest, June 2004
7. JWC and JFTC Training and Experimentation Facility AIS Concept User Requirements Analysis, Version: 1.1, December 2005
8. BI-SC 75–3 Collective training and Exercise Directive, Version: Latest, OKT 2010
9. MSG-068 NETN TAP, Version: Latest, April 2007
10. IEEE Standard 1516–2010, 2010
11. [HUI2009] Huiskamp, W., Wymenga, R., Krijnen, R. and Harmsen, E., Network Infrastructure Design Document for NATO Education and Training Network (NETN), June 2009
12. Training for success. Joint Training initiatives improve security in the Balkans – col. Orlin Nikolov, Per Concordiam vol.6, Issue 1, 2015

13. M&S Support for Crisis and Disaster Management Processes and Climate Change Implications, 2016, M.Sc. Tomov, N.- BULSIM, BULGARIA Asst. Prof. M.Sc. Nikolova, I. PhD., BAS, col. Orlin Nikolov, CMDR COE
14. Building Societal Resilience against hybrid Threats, Orlin Nikolov, Information and Security: An international Journal, v.39:1, 2018, 91–110
15. Support Decision Makers in Crisis and Disaster Management, Orlin Nikolov, ITEC Conference 2018
16. M&S decision making support for Crisis Disaster Management & Climate Change Implications, Orlin Nikolov, Kostadin Lazarov, NMSG Symposium 2020
17. Joint Training for success, Concordiam, Vol.6, issue 1, 2015 18–25
18. Vaklinova, Gergana. 2019. Tracing resilience – a context of uncertainty, a trajectory of motion. CMDR COE Proceedings. 2019, p. 12–13. <https://www.cmdrcoe.org/download.php?id=1587>

# Civil-Military Cooperation for the Countering of Threats: Protection of Civilians During the Development of a Threat



M. Stette, K. Porath, and S. Muehlich

## 1 Introduction

Having a strong military is fundamental to our security, but our military cannot be strong if our societies are weak; so our first line of defence must be strong societies able to prevent, endure, adapt, and bounce back from whatever happens. (NATO Secretary General Jens Stoltenberg, 07.10.2020 Global Security Bratislava Forum)

A robust resilience of member states, as called for by NATO Secretary General Jens Stoltenberg in his speech at the “Global Security Bratislava Forum”, is essential for NATO’s collective security and defence. Each NATO member must be resilient to withstand and recover quickly from a major shock such as a hybrid or armed attack, a natural disaster, a health crisis (including pandemics), or the failure of critical infrastructure.<sup>1</sup> Resilience is therefore described as the ability of a nation to withstand and recover easily and quickly from such challenges, combining civil preparedness as well as military capabilities.<sup>2</sup> The concept of resilience is not a disruptive or revolutionary new development in NATO. On the contrary, resilience has been present since NATO’s founding and is an important part of the 3rd Article of the Washington Treaty: “In order more effectively to achieve the objectives of

---

<sup>1</sup> Stoltenberg, J. 2021, p. 3.

<sup>2</sup> NATO Public Diplomacy Division 2021, p. 1.

---

M. Stette

BwConsulting – Inhouse Consulting of the German Armed Forces, Berlin, Germany

K. Porath (✉) · S. Muehlich

Concepts, Interoperability, Capabilities, Civil-Military Cooperation Centre of Excellence, Den Haag, The Netherlands

e-mail: [porath.k@cimic-coe.org](mailto:porath.k@cimic-coe.org); [Muehlich.s@cimic-coe.org](mailto:Muehlich.s@cimic-coe.org)

this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack”.<sup>3</sup>

During the Cold War, the maintenance and further development of resilience (or civil emergency preparedness) in NATO countries were firmly anchored in the organizational and command structures and were promoted as an objective with the necessary resources. With the supposed “end of history”<sup>4</sup> in the mid-1990s, an eminent part of the resilience planning of NATO and the member states was shelved, and the necessary resources and capabilities were substantially reduced. Only the annexation of Crimea in 2014 by the Russian Federation in violation of international law led to a change in the security paradigm that had been in place since the end of the Cold War. This prompted NATO to focus more on its core functions of defence and deterrence. As a result, there has been a renewed focus on strengthening the Alliance’s resilience as today’s threats of a hybrid or terrorist nature increasingly target society itself or critical infrastructure.<sup>5</sup> As recently as 2016, the North Atlantic Council committed to rebuilding resilience at the Warsaw Summit: “We are today making a commitment to continue to enhance our Resilience against the full spectrum of threats, including hybrid threats, from any direction. Resilience is an essential basis for credible deterrence and defence and effective fulfilment of the Alliance’s core tasks.”<sup>6</sup> The commitment is part of NATO’s response to the changing security paradigm and fits into NATO’s deterrence policy. The emergence of complex, nontraditional threat scenarios (military and non-military) such as cyberattacks or “hybrid warfare” led NATO to recognize that the protection of critical infrastructures, basic civilian services, and society itself is the first line of defence for today’s modern societies, as well as the basis for NATO’s military capabilities and readiness. Based on these findings, the “Baseline Requirements for National Resilience” were adopted. These form the backbone of national resilience and pursue the goal of making NATO member states more resilient.<sup>7</sup> In 2020/2021, COVID-19 clearly demonstrated the world’s vulnerability, including NATO’s, particularly with regard to its resilience. Above all, the realisation emerged that NATO’s resilience must include not only state institutions and the economic sector but also civil societies.

Societal resilience has been a relatively uncharted literature field. There are a lot of papers, books, and contributions to resilience in general but not about the social aspects and perspectives in the military field of action. The increasing level of attention to societal resilience indicates its growing relevance for NATO and its member states. Therefore, this study deals specifically with the research question:

---

<sup>3</sup> NATO 1949, The North Atlantic Treaty, p. 1.

<sup>4</sup> Fukuyama, F. 1992, p. 80.

<sup>5</sup> Roepke, W.-D. & Thankey, H. 2019, pp. 2 et seq.

<sup>6</sup> Prior, T. 2017, p. 1; NATO 1949, The North Atlantic Treaty, p. 1.

<sup>7</sup> Roepke, W.-D. & Thankey, H. 2019, pp. 2 et seq.

What can NATO and its entities do to strengthen the Societal Resilience of its member states?

## 2 Explanation of Resilience

### 2.1 Resilience and Societal Resilience in General

For some years now, the term resilience has been an absolute fashion and buzzword.<sup>8</sup> The COVID-19 pandemic has reinforced this trend even further. Nevertheless, the term itself is not new. As early as the 1940s and 1950s, the term resilience was used in the research field of psychology (although other sources report that the term was first used in the field of ecology) to describe how people deal with unexpected, personal, and severe strokes of fate.<sup>9</sup> It became apparent that resilience's underlying ability to withstand or overcome (abrupt) crises and shocks and thus maintain essential functions is the lowest common denominator of the traditional meaning of the term resilience.

In the following decades, the concept was taken up by a large number of other scientific disciplines (economics, engineering, social sciences, and humanities) and policy fields (development and climate policy, civil protection/security policy). Consequently, the concept of resilience has been further developed and differentiated (e.g. different categories of analysis: Individual, local, regional, state, societal, organizations, etc.).<sup>10</sup>

In the American Journal of Community Psychology, resilience has been defined more generically as: "a process that combines a set of adaptive skills with positive functional and adaptive development following a shock or disruption".<sup>11</sup> This definition implies that resilience is a process but can also be seen as a strategy or the "ability of a system to maintain its functions and structure in the face of internal and external change".<sup>12</sup>

It is apparent that the term resilience is used in a wide variety of scientific research fields. However, this means that there is no generally valid definition of the term. On the contrary, the ever-increasing number of divergent definitions leads to contradictions between individual interpretations and thus to an increasing dilution of the overall concept. As a result, it is becoming increasingly difficult to translate theory into practice and to pinpoint the goals, strategies, instruments, and actors involved in strengthening resilience. While there is majority agreement that resilience is not a dichotomous concept, the question of how different degrees of

---

<sup>8</sup> Brown, K. 2015, p. 28.

<sup>9</sup> Hanisch, M. 2016, p. 1; Pernik, P. & Jermalavičius, T. 2016, pp. 1 et seq.

<sup>10</sup> Hanisch, M. 2016, p. 1.

<sup>11</sup> Norris, F.H. et al. 2008, p. 130.

<sup>12</sup> Pernik, P. & Jermalavičius, T. 2016, pp. 1 et seq.

resilience can be measured remains unanswered. The term resilience thus not only runs the risk of degenerating into a mere buzzword but could also raise false hopes and expectations of being a panacea against all kinds of challenges.

Built on those views, societal resilience needs further explanation.

Based on Versteegden's comprehensive and inclusive model, societal resilience consists of seven indicators. A resilient society is characterized by high social capital, interconnectivity, trust, values and norms, narratives, innovation and education, and forewarning or awareness of a threat.<sup>13</sup>

For Rodin, social capital is an important indicator of societal resilience. It describes the extent to which the citizens of a state are rooted in communities. These communities can be all kinds of civil society or voluntary organizations, associations, or even neighbourhoods. The result of these communities is "the glue that holds people together" and leads to a common commitment, identity, and shared values and opinions.<sup>14</sup> Closely related to social capital is the aspect of interconnectivity. A resilient society requires the ability to cooperate deeply and sustainably whether it is internally or externally. One example of this is the cooperation between the state, the private sector, and society to strengthen societal resilience.<sup>15</sup> To weaken disinformation campaigns and the polarization of society, trust is essential for societal resilience.<sup>16</sup> For Versteegden, trust is the willingness of citizens to be vulnerable combined with a positive expectation for the future. Political trust is further defined as the willingness of citizens to be vulnerable to the actions of their government in the face of the uncertainties of the future, in return for which citizens assume that the government will adhere to ethical principles in its dealings with them (telling the truth, etc.).<sup>17</sup> According to Granelli, trust is the most important factor in effective strategic communication.<sup>18</sup> To identify values and norms, Versteegden states, Rodin elucidates some of the characteristics of resilience (e.g. politics, values, norms, behaviour, and identity). According to Durodié, it is what aligns society. Shared values and norms align society towards a goal and what is necessary to win the hearts and minds of the population. Thus, a resilient nation is based on shared values and norms. Narratives are also to be seen in this context; they are listed as a single aspect in the area of societal resilience, although they are definitely closely linked to values and norms. Narratives are a vehicle for conveying norms and values. They serve to create a framework of order and structure for the citizens of a state. "Innovation and education" are another important building block for societal resilience. In other words, innovation means "making things better / new". This is essential in order to develop innovative strategies that make it possible to deal appropriately with new types of threats. Equally important in this context is a

<sup>13</sup> Versteegden, C. 2018, pp. 25 et seq.

<sup>14</sup> Rodin, J. 2014, pp. 193 et seq.

<sup>15</sup> Versteegden, C. 2018, pp. 25 et seq.

<sup>16</sup> Bakker, E. & De Graaf, B. 2014, p. 15.

<sup>17</sup> Versteegden, C. 2018, pp. 25 et seq.

<sup>18</sup> Granelli, F. 2018, p. 201.

high level of education in society. Well-educated populations are significantly more resilient to disinformation campaigns, for example. The last indicator of societal resilience, forewarning, and awareness of a threat, refers to the fact that a society can only become more resilient if it identifies the threats it faces. This factor is all the more important because adversarial forces today increasingly rely on the surprise element of a strategic shock. Therefore, Versteegden characterizes resilient societies as being able to anticipate adversary actions and have functioning early warning systems in order to be able to react in time.

Although this societal resilience model according to Versteegden is a very comprehensive model, there is one central point of criticism. The individual aspects cannot be clearly distinguished from one another.

One example is the link between interconnectivity and social capital.<sup>19</sup>

### **3 Genesis and Strategic Context of NATO's Resilience Policy**

#### ***3.1 NATO Resilience: History***

While NATO speaks of resilience today, the term “civil emergency planning” dominated during the Cold War. In essence, however, both terms are aimed at the same mission: protecting the populations of NATO member states against the entire spectrum of potential threats (natural disasters, political concerns, armed conflicts, pandemics, etc.). During the Cold War, the focus was naturally more on military conflicts and natural disasters.

Civil emergency planning thus ensured that enough resources would be available in the event of a crisis and that these would be adequately distributed in order to minimize the impact on the state and the population. In this context, not only essential industrial and agricultural goods were considered but also human and transport capacities. The implementation of these civil protection measures would then have been carried out jointly by national, regional, and local authorities and services.<sup>20</sup>

Just as the legal basis for NATO's resilience today is based on Article 3 of the Washington Treaty, so it was for civil emergency planning. Even at NATO's establishment, it was clear that future wars would have to consider not only the military consequences but also the impact on the Alliance's population. A weak or vulnerable population would have opened up the possibility for an adversary to exploit and attack these vulnerabilities. Therefore, the protection of the population was given equal importance to military operations in NATO planning. These considerations were institutionalized in the 1950s under the Civil Emergency

---

<sup>19</sup> Versteegden, C. 2018, pp. 25 et seq.

<sup>20</sup> Van Heuven, M. 1970, pp. 1 et seq.

Planning Programme.<sup>21</sup> In the course of the Cold War, NATO member states, therefore, developed distinctive civil defence structures based on Article 3.<sup>22</sup>

The Civil Emergency Planning Committee (CEPC), which was created in the course of the Civil Emergency Planning Programme, was and is responsible for the policy guidelines, and is still the highest NATO authority in the field of civil emergency preparedness. The members of the Committee consist of representatives of the NATO member states responsible for their respective national civil emergency preparedness. In its original structure, the CEPC was chaired by eight planning groups dealing with different fields of civil emergency preparedness (Civil Aviation Planning Committee, the Civil Communications Planning Committee, the Civil Defence Committee, the Food and Agriculture Planning Committee, the Industrial Planning Committee, the Petroleum Planning Committee, the Planning Board on European Inland Transport, and the Planning Board on Ocean Shipping).

Today, the CEPC reports directly to the North Atlantic Council, NATO's highest policy-making body. The current structure consists of only four working groups: Transport Group, Civil Protection Group, Industrial Resources and Communications Group, and the Joint Health Agriculture and Food Group. The CEPC is supported by international staff at NATO headquarters in Brussels. In addition, the CEPC has access to a pool of more than 400 civilian experts who can be deployed to NATO (Partner) countries for support in the event of a strategic shock or for training purposes.

NATO's functions at the beginning of the Cold War in the field of civil emergency preparedness included above all a coordinative role. NATO was to regulate the exchange of information between the individual member states. Furthermore, so-called wartime agencies were developed to coordinate the actions of NATO countries in the event of war in the areas of Transport, Industry, Agriculture, and Civil Defence.<sup>23</sup> By the end of the 1980s, therefore, NATO had plans for eight such agencies, which could be activated if necessary.<sup>24</sup> In addition, the "Policy on Cooperation for Disaster Assistance in Peacetime" was adopted in 1958. In addition to the approach focused primarily on military conflicts, NATO thus developed a mechanism for responding quickly and effectively to (natural) disasters. Since then, this policy has been further developed twice (1971, 1993). In 1998, the NATO Disaster Assistance Policy underwent a complete overhaul and was massively redesigned. The clearest expression of this change process was the establishment of the Euro-Atlantic Disaster Response Coordination Centre (EADRCC). Today, the EADRCC acts as the central coordinating body for civil emergencies/major disasters in the Alliance and organizes requests for assistance and support to NATO members.<sup>25</sup> With the end of the Cold War and the associated disappearance of the

<sup>21</sup> CEPC 2016, Report on Enhancing Resilience through Civil Preparedness; CEPC 2016, Report on the State of Civil Preparedness.

<sup>22</sup> Van Heuven, M. 1970, pp. 1 et seq.; NATO 2021, Resilience and civil preparedness – Article 3.

<sup>23</sup> Van Heuven, M. 1970, pp. 1 et seq.

<sup>24</sup> Jacuch, A. 2020, pp. 274 et seq.

<sup>25</sup> Kufčák, J. & Matušek, T. 2017, p. 2.



direct threat from the Soviet Union or the Warsaw Pact and NATO's increasing focus on out-of-area operations, most NATO member states significantly reduced their commitment in the area of civil emergency preparedness. Since emergency preparedness in the member states was based primarily on civilian capacities that were in state hands and could be quickly mobilized for defence purposes in the event of a crisis, most countries had extensive potential for liberalization in this area. Consequently, this led to a wave of privatization of critical or strategic infrastructures and the outsourcing of former military capacities. From the 1990s onwards, the majority of civilian resources that play an important role in national security, such as energy and communications infrastructure or transportation, have therefore been in private sector hands.<sup>26</sup>

The return to more resilient structures was only discussed in the NATO context with the increased emergence of nonconventional threats such as terrorism. In the early 2000s, however, the scope of consideration for civil emergency planning was much narrower than it is today and related primarily to threats in the CBRN (chemical, biological, radiological, and nuclear) domain and to critical infrastructure protection.<sup>27</sup>

### ***3.2 The Annexation of Crimea in 2014 or Why NATO Is Again Concerned with Resilience***

With the annexation of Crimea by the Russian Federation under President Putin in violation of international law, Russia openly opposed the Western world.<sup>28</sup> Harbingers of these developments, such as Putin's speech at the Munich Security Conference in 2007, in which he strongly criticized the supremacy of the USA,<sup>29</sup> and the subsequent intervention in Georgia in 2008, were not taken seriously in the Western centres of power. Consequently, the incipient upheaval in the prevailing security paradigm in Europe was not recognized by Western policy planners.

The annexation of Crimea, therefore, provided an all the more bitter awakening. The violation of Ukraine's national sovereignty against the rules of international law caused massive concerns in the Baltic states and Poland, which now also see their political and territorial sovereignty as severely threatened.<sup>30</sup>

The post-Cold War model of Russia as a strategic partner of the West, based on the successful European integration of Russia and the concomitant creation of a Greater Europe from Lisbon to Vladivostok, is no longer conceivable since 2014.<sup>31</sup>

---

<sup>26</sup> Garriaud-Maylam, J. 2021, p. 3.

<sup>27</sup> Garriaud-Maylam, J. 2021, p. 3.

<sup>28</sup> Zum Felde, R.M. 2018, p. 1.

<sup>29</sup> Putin, V. 2007.

<sup>30</sup> Zum Felde, R.M. 2018, p. 2.

<sup>31</sup> Trenin, D. 2018, p. 1.

Today Russia is no longer a partner but an adversary in a potential conflict in Eastern Europe. The annexation of Crimea has impressively shown what the Russian armed forces are capable of despite a relatively short preparation time. The right conclusions have obviously been drawn from the lessons of the Georgia conflict. Whereas in 2008 a poorly equipped and poorly trained conscript army went into the field, in 2014 the modernized and capable Russian army was able to muster a full range of operations.<sup>32</sup> Above all, the means of unconventional warfare devised by Russia stood out.

With the illegal attack and invention and war against Ukraine, Russia has proven to be a significant threat to peace and stability in Europe. Although the duration of the conflict and how it has been developing are food for discussions about the capabilities and capacities of the Russian armed forces, this is not further considered in this document.

Hybrid warfare is a combined approach of conventional and unconventional means of warfare. That includes all instruments of power and thereby a “whole of government warfare”, i.e. warfare that is carried out by all government institutions and does not only include the traditionally responsible government agencies. This means that hybrid warfare includes military and intelligence elements as well as political, economic, and sociocultural elements. It can even go beyond unconventional to irregular warfare by applying illegal and nonattributable actions against an adversary, for example, disinformation campaigns, cyberattacks, polarization of societies, economic pressure, use of irregular (military) forces, etc. From an international law perspective, this way of hybrid warfare transcends war and peace and is thus legally located in a grey area. This makes an appropriate response to any activities in this spectrum challenging. Eugene Rumer of the Carnegie Endowment for International Peace, therefore, describes hybrid warfare as “permanent conflict”.

The Kremlin is thus in a position to exploit short-term opportunities (internal political unrest, for example) in the region using hybrid warfare while fighting a regional high-intensity conflict with a significant conventional dimension. The Baltic states and other NATO states (and also European Union (EU) states), which are in direct geographical proximity to Russia, see themselves put under massive pressure by these developments.<sup>33</sup>

As early as September 2014, the first steps were therefore taken to improve NATO’s deterrence and defence capabilities (“NATO Readiness Action Plan”). In this context, NATO examined the resilience of its member countries in a large-scale study.<sup>34</sup>

---

<sup>32</sup> Zum Felde, R.M. 2018, p. 3.

<sup>33</sup> Rumer, E. 2019, pp. 2 et seq.

<sup>34</sup> Meyer-Minnemann, L. 2016, pp. 3–8.

### ***3.3 The Risks of Modern Societies from a NATO Perspective***

Through the comprehensive analysis of the resilience of NATO countries, various relevant trends and developments have been identified. Thus, it became apparent that NATO's military forces are more dependent than ever on civilian capabilities and infrastructure capacities to ensure their operational readiness. Referring to Khan, 90% of military transport, 70% of military satcom, 75% of host nation support, and 85% of military requirements for food and water resources are from civilian and commercial sectors. In order to ensure that NATO forces have access to these capabilities and capacities, it is logical that functioning resilient structures are needed in the member states. The analysis has shown that civilian structures and infrastructures are not comparable to military structures in terms of their level of protection. They are vulnerable to attacks from the outside or susceptible to internal disruption. This makes it attractive for potential adversaries to exploit these vulnerabilities. As a result, NATO forces could be attacked indirectly, but, more importantly, the backbone of our societies, the civilian infrastructure, could become the main target.<sup>35</sup>

In general, it was found that today's societies are highly complex systems based on the functioning of critical infrastructures, which need to be able to withstand disruptions, whether internal or external. It is observed that the supply of resources and goods is dominated by purely market-based logic. The "just-in-time model" characterizes supply chains and has little to no redundancy. There is also the aspect of technological change: in our information age, the societies of NATO member states are interdependently linked, whether economically or socioculturally (however, this also applies to potential systemic rivals such as Russia and China). On the one hand, this interconnectedness creates efficient, cost-effective, and innovative synergies for our societies. On the other hand, it creates dependencies and vulnerabilities that potential adversaries can exploit. Consequently, the three main actors in resilience could be identified (the government, the private sector, and society).<sup>36</sup>

### ***3.4 The Warsaw NATO Summit 2016***

As part of the adaptation process to the changed security paradigm (besides the central aspect of hybrid warfare, strategic shocks were considered such as natural disasters, terrorism, climate change, pandemics, conventional wars, etc.) and the new threat situation to NATO's eastern flank, the North Atlantic Council adopted the Commitment to Strengthen NATO resilience in 2016. In this context, the seven

---

<sup>35</sup> Khan, J. 2019, p. 10.

<sup>36</sup> NATO 2021, Emerging and Disruptive Technologies.

BLRs were adopted by the heads of state and government of the NATO member states. These are discussed in detail in the next section.

The Warsaw Summit Communiqué describes NATO's relationship to resilience in two essential points. It describes resilience as the basis for NATO's deterrence capabilities and the fulfilment of its core tasks. Second, the Communiqué makes clear that, in order to be prepared against the full range of threats, NATO member states must better protect their civilian infrastructure and capabilities. This requires an integrated approach that encompasses all government institutions and the private sector.<sup>37</sup> The Warsaw Summit Decision contains a number of other points that have a major impact on the resilience of NATO member states. It makes clear that, in addition to strengthening processes, structures, and systems, it is above all the shared values and narratives of NATO member states that provide effective protection against, for example, hybrid warfare. Our democratic system, governance, individual personal freedom, and the rule of law are among our most important lines of defence. The communiqué goes on to say that resilience-building is first and foremost a national responsibility. Therefore, NATO's role in this field is mainly supportive. This means that there can be no generally applicable solution for strengthening resilience but that each state must design and implement its own system individually, adapted to its given national framework conditions. This is intended to maintain a certain degree of flexibility and enable the demands of other actors, such as the European Union, to be met in this policy field. This goes hand in hand with the last point of the Warsaw Decision. NATO's resilience is to be strengthened through effective cooperation with other actors, in particular with the EU. The same applies to the strengthening of resilience in partner states in the Alliance's neighbourhood for example Ukraine, Sweden, and Finland.<sup>38</sup>

In order to assess the state of the resilience of member states, NATO compiles a report on the state of civil preparedness every 2 years.<sup>39</sup>

### ***3.5 The COVID-19 Pandemic and Societal Resilience***

The current COVID-19 pandemic offers valuable insights in how to deal with challenges that do not threaten the "classic" military security of Alliance member states but nevertheless have the potential to destabilize entire societies. Therefore, the pandemic is an important test of NATO's resilience to the full spectrum of threats.

---

<sup>37</sup> NATO 2016, The Warsaw Declaration on Transatlantic Security; NATO 2021, Strengthened Resilience Commitment.

<sup>38</sup> NATO 2016, The Warsaw Declaration on Transatlantic Security; NATO 2021, Strengthened Resilience Commitment.

<sup>39</sup> NATO 2021, Civil Preparedness.

In considering the COVID-19 pandemic and its impact to date, one thing has become clear: the civilian populations of NATO member states are one of the most important stakeholders of resilience and have been almost completely overlooked in resilience-building efforts in recent years. Yet the vast majority of actions directed against NATO today are aimed at one thing above all – influencing the population. The example of the COVID-19 pandemic illustrates this particularly well. The effectiveness of protective measures against Corona depends primarily on whether and to what extent the citizens of NATO countries accept and internalize them. This requires trust in local, regional, and national structures. Consequently, it was found that societies that have a higher level of trust in their population in their governments and state structures, regardless of the political system, have more success in the fight against the pandemic than societies that have only a low level of trust in them.<sup>40</sup>

A recent report by the European External Action Service has now confirmed that opposing forces are using disinformation campaigns to undermine this relationship of trust and promote the polarisation of targeted societies.<sup>41</sup>

In order to withstand and counteract these campaigns and the resulting loss of trust and polarization, well-educated and informed citizens are needed. For this, free and independent media/information combined with science-based educational programmes for the population is essential. This also includes, for example, information on how citizens can best prepare themselves for a crisis. Such initiatives have already been implemented in Germany, Estonia, Latvia, Lithuania, and designated NATO nations Sweden and Finland. Finland is also starting to raise children's awareness of disinformation as early as primary school.

Ultimately, NATO's experience with the aftermath of the COVID-19 pandemic, among other factors, demonstrates that building societal resilience is essential.

### ***3.6 The Brussels NATO Summit 2021***

In December 2019, NATO Heads of State and Government tasked Secretary General Stoltenberg with strengthening NATO's political dimension. In this context, several proposals were drawn up under the title "NATO 2030" to best prepare NATO for the challenges of the future. Specifically, the proposals include maintaining the Alliance's military strength, promoting the Alliance's political dimension, and allowing NATO to implement a more global approach.<sup>42</sup>

These proposals formed the core of the measures adopted by the political decision-makers of the NATO member states in Brussels on 14 June 2021. Within these measures, the further strengthening of NATO's resilience plays a central role. Consequently, the "Strengthened Resilience Commitment" was adopted in

---

<sup>40</sup> CCOE CIMIC Messenger 2020, pp. 4 et seq.

<sup>41</sup> European External Action Service 2021, pp. 1 et seq.

<sup>42</sup> Stoltenberg, J. 2021, p. 2.

the course of the Brussels Conference. This aims to ensure that member states implement an even better coordinated and more comprehensive approach to NATO resilience. This means that in addition to NATO's "whole of government" approach, private sector actors, nongovernmental organizations, and the societies of NATO's members are to be more involved ("whole of society"). In addition, the Allies agreed to further develop the NATO resilience goals. These will be operationalized through national goals as well as supported by national implementation plans. These alliance goals and activities will be reviewed as part of a newly created resilience evaluation cycle.<sup>43</sup> In this way, they can act as guidelines for the individual-national protection goals and at the same time provide more clarity and comparability within the Alliance.

Other important points of the Brussels Summit decision include a lessons-identified/lessons-learned analysis from the experience of the COVID-19 crisis and the assurance that promoting resilience is first and foremost a national responsibility. In addition, NATO decided to improve the protection of critical infrastructure and key supply chains and to strengthen cooperation with partner organisations, first and foremost the European Union. It also sent a strong message in defence of the shared value principles of individual freedom, democracy, human rights, and the rule of law.<sup>44</sup> It turns out that resilience is not a revolutionary or new issue for NATO. Article 3 of the Washington Treaty as the basis for all NATO efforts in this area, the peak of civil defence efforts during the Cold War, the peace dividend in 1990/2000, and finally the changing security paradigm after the Crimea annexation lead us to today's NATO resilience policy. The 2016 and 2021 Commitment of Heads of State and Government and the COVID-19 pandemic have highlighted the importance of building resilience.

Based on the Brussels Summit Resolution and the ambitions defined in the NATO 2030 Concept, an even more coordinated and integrated approach needs to be developed in the area of Resilience through Civil Preparedness (RtCP). Various measures have been developed for this purpose. Each member state was asked to select a high-level national contact person to coordinate efforts to promote resilience. It was also decided to develop the CEPC into a "Resilience Committee" to reflect the increased importance of resilience in the organization.

As briefly outlined above in the previous chapter, alliance-wide resilience goals are to be developed. These will be operationalized through national goals as well as supported by national implementation plans. These alliance goals and activities will be reviewed as part of a newly created resilience evaluation cycle.<sup>45</sup>

It is likely that these developments will be reflected in NATO's new Strategic Concept, which will be adopted in Madrid, Spain, in the summer of 2022. NATO's Strategic Concept lays the foundation for the Alliance's future political and military development and provides guidance on security challenges. The Concept underpins

---

<sup>43</sup> CEPC 2022, Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria.

<sup>44</sup> NATO 2021, Strengthened Resilience Commitment.

<sup>45</sup> CEPC 2022, Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria.

NATO's purpose, character, and fundamental missions. Since the security situation is in a state of slow but constant change, the Strategic Concept is subject to a regular revision process. This ensures that NATO, as a self-transforming organization, is able to deal effectively with new security challenges. In addition, a decision was taken last year to strengthen NATO's military resilience as part of the NATO Warfighting Capstone Concept. An initial concept for layered resilience has already been drafted in the course of a workshop week at the CCOE together with experts. In contrast to RtCP, however, it is not the CEPC (Resilience Committee) that is in charge but the Allied Command Transformation in Norfolk.

## **4 NATO's Understanding of Resilience and Societal Resilience**

### ***4.1 Definition and Stakeholder***

First of all, it should be noted that there is no official NATO definition of resilience. This is due to several reasons: on the one hand, the lack of a definition provides flexibility in the orientation of the policy; on the other hand, it is primarily due to the fact that NATO member states have not yet been able to agree on an official definition, although there is a basic agreement on what resilience means for NATO. Nevertheless, there are some working definitions such as from Allied Command Operations or the Civil-Military Cooperation Centre of Excellence. These definitions describe resilience as being able to withstand strategic shocks and recover easily and quickly from them. Resilience combines civil and societal emergency preparedness as well as military capabilities.<sup>46</sup> Resilience is an adaptive process in which the performance of the system is defined by absorbing strategic shocks with minimal impact. At the same time, essential functions of the system are maintained at a sufficient level to then restore functionality in a reasonable time and at a reasonable cost. While preparation for strategic shocks is an integral part, these shocks themselves are usually unpredictable and unavoidable. Therefore, a resilient system focuses specifically on managing the consequences of a shock and isolating the event from the function of the overall system. In the final phase, the system evolves and adapts, increasing its capacity to withstand future similar strategic shocks. In several speeches, articles, and lectures, the final phase describes the "bounce-back" effect.<sup>47</sup> This term is taken from the general Resilience literature.<sup>48</sup>

---

<sup>46</sup> CCOE 2021, Resilience through Civil Preparedness; Stoltenberg, J. 2021, p. 3; NATO Public Diplomacy Division 2021, p. 1.

<sup>47</sup> Roepke, W.-D. & Thankey, H. 2019, pp. 2–8.; Stoltenberg, J. 2021, p. 3; CCOE 2021, Infosheet Resilience through Civil Preparedness.

<sup>48</sup> Smith, B.W. et al. 2010, p. 194.

## Stakeholders

In the following, the three most important stakeholders of the NATO resilience policy: the government and its institutions, the private sector, and society are briefly described and their roles are outlined. This ensures the necessary contextualization of the overall field of resilience in NATO.

- Government

The national, regional, and local state structures in the member states are primarily responsible for building resilience. In doing so, they create the legal and institutional framework that underpins a resilient nation. In addition, they are responsible for providing and coordinating the distribution of financial and other resources needed for crisis preparedness and direct crisis response. Official authorities bear responsibility for crisis communication; this applies both in preparedness and in the crisis response itself.<sup>49</sup> In the area of preparedness, other actors are empowered to contribute to national resilience through targeted communication such as brochures (“What do I do in case of a crisis”). Prominent examples of countries with such public information campaigns would include Sweden and Norway.<sup>50</sup> In the crisis itself, the government at all levels must ensure that citizens receive prompt, accurate information. This increases trust in the government and its actions and at the same time inhibits disinformation campaigns.<sup>51</sup>

- Private sector

Resilience is a task not only for government authorities but also, and above all, for the private sector. Today, private sector companies operate the vast majority of the critical infrastructures that form the backbone of our societal structures. They also produce the goods that not only keep our daily lives running but also enable the deployment of NATO forces. Therefore, it is essential to engage the private sector in promoting resilience. Additionally, it is necessary to closely monitor foreign direct investment in critical infrastructure and strategic sectors of the economy. The growth of such investments by strategic rivals on the global political stage, in the event of a crisis, could harm the resilience of NATO member states. The public and private sectors must work closely together, in this case, to identify potential vulnerabilities and develop appropriate plans to maintain core structures.<sup>52</sup>

In this context, it is important that companies promote their own crisis resilience and thus ensure that critical areas of their business model are able to continue operating under the pressure of a crisis – “business continuity planning”. This is particularly true with regard to the aspect of increasing dependence on information technology.<sup>53</sup>

---

<sup>49</sup> Garriaud-Maylam, J. 2021, p. 4.

<sup>50</sup> Braw, E. 2021, p. 8.

<sup>51</sup> Garriaud-Maylam, J. 2021, p. 4.

<sup>52</sup> Garriaud-Maylam, J. 2021, p. 4.

<sup>53</sup> Cabinet Office UK, The National Resilience Strategy 2021, p. 22.



- Society

The population of NATO member states is the third stakeholder in resilience and at the same time the most neglected. Yet the vast majority of threats today are directly aimed at damaging or destabilizing our societies. On the other hand, a resilient population provides the first line of our defence against the full spectrum of threats.<sup>54</sup> Therefore, it is essential to put the people or the population at the centre of the promotion of national resilience. This can be done through various measures such as information campaigns on how to deal with crises, the creation of exercises and training for civilians, the inclusion of educational content on resilience in schools, etc.<sup>55</sup>

In the context of NATO, societal resilience is not a new perspective on resilience in general. However, the focus of NATO's resilience agenda in recent years has been primarily on the first two key stakeholders. It was not until the COVID-19 pandemic that society, respectively, returned to the centre of attention. Based on the experience of COVID-19, NATO identified several areas of action that are particularly relevant for strengthening the societal resilience of its member states: movement and border crossing restrictions; public messaging about government responses; ensuring public access to transparent, timely, and accurate information to counter disinformation; and the availability of critical personnel for essential services.<sup>56</sup>

## ***4.2 Resilience Through Civil Preparedness***

### **The Seven Baseline Requirements**

Based on the continuity of government, continuity of essential services to the population, and civil support to military operations, the BLRs were adopted at the 2016 NATO Summit in Warsaw and updated in 2020 and 2021 to reflect the lessons learned from the COVID-19 pandemic and the impact of emerging disruptive technology. The BLRs reflect a “whole of government” approach. This means that all relevant government institutions must participate in the design, implementation, and further development of resilience. In doing so, the BLRs support the fulfilment of the central objectives of civil preparedness.<sup>57</sup>

NATO defines civil emergency preparedness as follows: “the ability to maintain functions vital to society, to ensure the basic needs of the population and the state's ability to act in a crisis situation, and to ensure support for the armed forces in the event of war or crisis”.<sup>58</sup> Well-developed societal competencies in critical

---

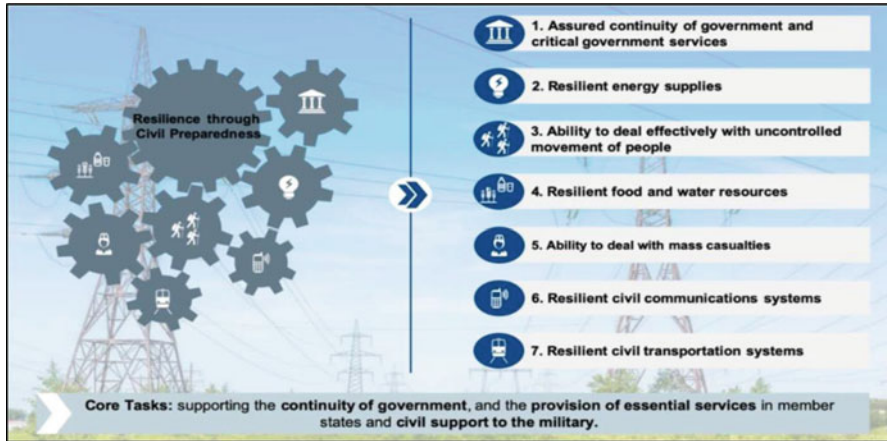
<sup>54</sup> Cabinet Office UK, *The National Resilience Strategy* 2021, p. 22.

<sup>55</sup> Braw, E. 2021, pp. 7 et seq.

<sup>56</sup> CEPC 2020, *Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria*.

<sup>57</sup> NATO 2021, *Strengthened Resilience Commitment*.

<sup>58</sup> Ministry for Foreign Affairs of Finland 2021, pp. 1 et seq.



**Fig. 1** Baseline requirements and core tasks. (Own illustration according to CEPC 2020, pp. 1–30)

thinking lead to a more resilient society. This competence, in combination with a high level of trust in the political system, the integrity of political leadership, and extensive and transparent government communication, enables the identification and management of hostile propaganda, misinformation and disinformation, protest campaigns, and political extremism.<sup>1</sup> The presence of these factors reduces the likelihood of destabilizing actions by potential aggressors (Deterrence by Denial) (Fig. 1).<sup>59</sup>

### Criticism of the Baseline Requirements

Although the BLRs for national resilience are largely uncontroversial, there are some points of criticism. For example, it is a very state-centric approach. The focus is primarily on planning and preparing measures at a ministerial or subministerial level. Furthermore, institutions (states, NATO) are to be strengthened above all. This approach ignores the fact that a large part of the capacities and capabilities needed to fulfil the BLRs are in civilian hands, and therefore extensive cooperation with private sector actors is needed for successful resilience-building.<sup>60</sup> The same is true for the promotion of societal resilience. Civil society is reflected far too little in the BLRs as a relevant actor. Citizens need to be involved in strengthening national security. In addition, the focus on a top-down approach allows little flexibility in the implementation of the BLRs.<sup>61</sup>

<sup>59</sup> Mazarr, M.J. 2020, pp. 23 et seq.

<sup>60</sup> Townsend, J. & Agachi, A. 2020, pp. 1 et seq.

<sup>61</sup> Hoogensen Gjørø, G. 2020, p. 1.

### **4.3 NATO CIMIC and Resilience**

Civil-Military Cooperation (CIMIC) is a joint function providing NATO with essential capabilities in support of the achievement of mission objectives; specifically, CIMIC allows NATO commands to participate effectively in a broad spectrum of interactions with a variety of non-military actors within the area of operations.<sup>62</sup> Commanders are required to assess and analyse the civil environment during the planning and execution of military operations. As such, CIMIC activities are applicable to all types of NATO operations. Essentially, CIMIC's role is to ensure mission success by reducing the unintended negative impact that military operations can have on the civil environment and, conversely, the hampering impact that civilian activities can have on NATO operations. Specifically, CIMIC's goal is to contribute to mission success by supporting effects that influence and sustain favourable conditions in the civil environment. CIMIC therefore also has a role to play in enhancing NATO's resilience.<sup>63</sup> NATO CIMIC focuses on interactions and coordination with non-military actors as part of NATO's contribution to a comprehensive approach. NATO CIMIC is mandated with three core functions: Civil-Military Liaison, support to the force, and support to non-military actors and the civil environment.<sup>145</sup>

#### **Civil-Military Liaison**

Civil-Military Liaison is intended as the contact, intercommunication, and coordination maintained between elements of the military and other non-military actors to ensure mutual understanding and unity of purpose and action. The aim of the Civil-Military Liaison is to facilitate interactions, harmonize actions, share information, and support concerted or integrated planning and conduct of operations.<sup>64</sup> The military aims to achieve this through timely identification of key non-military actors that can contribute to the overall mission's success.<sup>65</sup>

#### **Support to the Force**

To minimize the risk of disruption to military operations, commanders will require non-military support from within their joint operations area. As the force may be dependent on civilian resources and sources of information, CIMIC contributes to the planning and execution of operations through cooperation with the civil envi-

---

<sup>62</sup> CCOE CIMIC Handbook 2019, p. 7.

<sup>63</sup> NATO Standardization Office 2018, p. 1<sup>145</sup> CCOE CIMIC Handbook 2019, p. 9.

<sup>64</sup> NATO Standardization Office 2018, p. 5

<sup>65</sup> CCOE CIMIC Handbook 2019, p. 9

ronment and other military functions.<sup>66</sup> Specifically, CIMIC contributes to mission success by gathering and reporting information on the civil environment to assess the impact of military operations on the local population and providing counsel on how to mitigate the negative consequences. Additionally, CIMIC promotes force acceptance among non-military actors by informing the civil society in the mission area in accordance with the strategic communication efforts.<sup>67</sup>

### **Support to Non-military Actors and the Civil Environment**

CIMIC will ensure the provision of military support to non-military actors and the civil environment only if it is required to create conditions favourable to mission accomplishment. In fact, CIMIC is not responsible to provide direct support to non-military actors, as its role is rather to liaise with non-military and other military actors to facilitate such support.<sup>68</sup>

## **5 Methodology**

This section describes the methodology, which “[...] can be regarded as the discipline of applying (and understanding) appropriate methods and processes for specific pieces of research”.<sup>69</sup> Starting with the research approach and design, this chapter deals with further steps of the research process in chronological order like the choice of expert interviews as the primary instrument, guideline development, type and criteria of sampling, and therefore the analysis and evaluation of this collected data in a longitudinal study.

### ***5.1 Research Approach and Design***

According to the kind of question and dependent methods to get information for answering the research question, interpretative qualitative research has been chosen (the “How and Why” focusing on inductive theories, using verification from observations<sup>70</sup>), focusing mainly on Kuckartz’s perspective and views to collect and analyse data.<sup>71</sup> In this respect, the study consists of mainly qualitative

<sup>66</sup> NATO Standardization Office 2018, p. 6

<sup>67</sup> CCOE CIMIC Handbook 2019, p. 10

<sup>68</sup> NATO Standardization Office 2018, p. 2.

<sup>69</sup> Almalki, S. 2016, p. 290.

<sup>70</sup> Mayer, H.O. 2013, p. 26; Kuckartz, U. 2014, p. 4; Almalki, S. 2016, p. 291; Rieker, P. and Seipel, C. 2006, p. 4041; Gioia, D.A. et al. 2012, p. 18; Terrell, S.R. 2012, p. 258.

<sup>71</sup> Creswell, J.W. 2014, p. 50.

interpretations, enriched by a specific number of conducted interviews. This kind of research is focusing on a variety of interpretations and content, following a longitudinal case study perspective with an ethnographic design.<sup>72</sup> The research design in particular is defined as being a “type of inquiry within these different approaches” as Creswell states.<sup>73</sup> Ethnographic design means in this context a qualitative method in which researchers observe or interact with participants in their real-life environment. That is necessary as the study wants to build “an in-depth, contextual understanding of the case, relying on multiple data sources rather than on individual stories as in narrative research” and relies on the specific environment of every single participant.<sup>74</sup> Every participant is differently related to NATO, which makes it valuable to reflect on their specific knowledge. In that sense, qualitative data symbolizes ‘richness and holism, with strong potential for revealing complexity [...] in a real context [...]’ as Miles and Huberman state.<sup>75</sup> The variety of instruments depends on the research approach and consists of primary and secondary tools. In this study, it was expert interviews and written down information about resilience and NATO-related documents.

Common literature describes two perspectives of the research’s focus. Either the approach is focused on a close connection to literature and the research question,<sup>76</sup> or it is kept as open as possible to not miss any information that could be useful in any matter at all.<sup>77</sup> Practical qualitative research like this study often lies between these two extremes. In having a formulated general research question along with a rudimentary conceptual framework and an idea of data-gathering, the research design is more tightly defined.<sup>78</sup> Therefore, the collection of data has to be selective for preventing an overload of information that compromises the efficiency and power of the analysis.<sup>79</sup> Following this design, the instrumentation (guiding questions) has to be well-structured and explicitly developed too.<sup>80</sup>

Generic quality criteria of qualitative research are much-discussed in literature.<sup>81</sup> As O’Reilly and Parker comment: “Furthermore, there is no singular way to measure the quality of qualitative research because it is so diverse”.<sup>82</sup> However, in contrast to quantitative research, methodologically controllable and reflective subjectivity might be the focus, as this study applies those criteria as well.<sup>83</sup> It is

<sup>72</sup> Creswell, J.W. et al. 2007, p. 241; Creswell, J.W. 2014, pp. 43, 236; Terrell, S.R. 2012, p. 257.

<sup>73</sup> Creswell, J.W. 2014, pp. 41, 295

<sup>74</sup> Creswell, J.W. et al. 2007, p. 245.

<sup>75</sup> Miles, M.B. and Huberman, A.M. 1994, p. 10.

<sup>76</sup> Miles, M.B. and Huberman, A.M. 1994, p. 17; Andresen, F. 2017, p. 120.

<sup>77</sup> Glaser, B.G. and Strauss, A.L. 1967, p. 365; Gioia, D.A. et al. 2012, p. 16; Andresen, F. 2017, p. 120; Miles, M.B. and Huberman, A.M. 1994, p. 17.

<sup>78</sup> Miles, M.B. and Huberman, A.M. 1994, p. 17

<sup>79</sup> Miles, M.B. and Huberman, A.M. 1994, pp. 17, 35, 55; Eisenhardt, K.M. 1989, p. 536.

<sup>80</sup> Miles, M.B. and Huberman, A.M. 1994, p. 35; Yin, R.K. 1992, p. 131.

<sup>81</sup> O’Reilly, M. and Parker, N. 2012, p. 191; Creswell, J.W. 2014, p. 251.

<sup>82</sup> O’Reilly, M. and Parker, N. 2012, p. 191.

<sup>83</sup> Helfferich, C. 2019, p. 683.

important to reflect the opinion of the participants without their own biases and finally interpret those results. Therefore, the questions needed to be clarified in advance for preventing any subjectivity. Other important criteria for the quality of qualitative research are consistency (qualitative reliability) and dependability (qualitative validity) of the results.<sup>84</sup> Other researchers have to be able to follow the structure and understand the research design and the accuracy of the findings by applying certain procedures.<sup>85</sup> That means the data collection and specific techniques of the analysis need to be described in detail. Focusing on the ability to get the same content as in quantitative research is not necessary as qualitative research relies on the context-related and interpretative nature of the design.<sup>86</sup> Nevertheless, using different sources and a transparent logical chain of evidence of collected data favours the construct validity in any way.<sup>87</sup>

## 5.2 Data Collection

There are many different tools within the interpretative approach in qualitative research like experiments, questionnaires/guidelines, or historical approaches, depending on the individual intention of the researcher.<sup>88</sup> The written word (archival records, transcripts of interviews, and field notes from direct observations) can be used as primary or secondary instruments for collecting data in different settings and was – in form of transcribed interviews – the main data source of this study.<sup>89</sup> This raw material needs to be further processed.<sup>90</sup> The final state of collecting data is to achieve confirmatory evidence or an answer to the research question, from at least two or more sources.<sup>91</sup> This is called “saturation”, the point when data collection reaches its peak and the researcher does not need any more information to solve the case and answer the question.

Since there is no sufficient data on this topic yet and literature is not well developed in this specific area, applying primary data collection instruments offered a good opportunity to collect information anew.<sup>92</sup> The open guided interview as

<sup>84</sup> Ruona, W.E.A. 2005, p. 247.

<sup>85</sup> Andresen, F. 2017, p. 111; Creswell, J.W. 2014, pp. 251, 260; Glaser, B.G. and Strauss, A.L. 1967, p. 365.

<sup>86</sup> Helfferich, C. 2019, p. 683; Ruona, W.E.A. 2005, p. 247; Glaser, B.G. and Strauss, A.L. 1967, p. 365; Bogner, A. et al. 2014, p. 72.

<sup>87</sup> Yin, R.K. 1992, p. 131; Andresen, F. 2017, p. 110; Helfferich, C. 2019, p. 683; Eisenhardt, K.M. 1989, p. 544.

<sup>88</sup> Andresen, F., 2017, p. 103.

<sup>89</sup> Andresen, F. 2017, p. 111; Yin, R.K. 1992, p. 131; Mayring, P. 2000, p. 3; Raediker, S. and Kuckartz, U. 2019, p. 2; Miles, M.B. and Huberman, A.M., p. 9; Creswell, J.W. et al. 2007, p. 247; Ruona, W.E.A. 2005, p. 234.

<sup>90</sup> Miles, M.B. and Huberman, A.M. 1994, pp. 9, 51.

<sup>91</sup> Andresen, F., 2017, p. 111.

<sup>92</sup> Miles, M.B. and Huberman, A.M. 1994, p. 10; Liebold, R. and Trinczek, R., 2009, p. 36.

an expert interview, in particular, functioned as the central and primary instrument for data collection in this study, as it is important to gain in-depth knowledge that is not written down yet. Rigid questionnaires are known for being relatively efficient and fast but also less reactive. Therefore, the open guided interview seemed the better option for conducting this research. Secondary research instruments are already available data, i.e. archival records, existing documents, or other already written down information. Due to the sensitive nature of the topic, a significant portion of NATO documents are classified and therefore not releasable to the public. For this reason, the theoretical part of this work is built on secondary data, focusing on NATO UNCLASSIFIED documents like summit decisions, requirements, guidelines, and conference reports.

Scientific papers and books, for example, by Mazarr<sup>93</sup> and Hamilton,<sup>94</sup> built the theoretical foundation for the construct of resilience in this study. Helfferich and Bogner et al. were one of the main sources in supporting the design of questions for the open guided interview.<sup>95</sup> The presentation of the evaluation of data, in particular, focused on the work of Kuckartz<sup>96</sup> and Mayring.<sup>97</sup> Huberman and Creswell were one of the main sources of designing the methodology of this research.<sup>98</sup> Using primary and secondary instruments and getting direct and indirect information is referred to as “data triangulation” (multiple data collection).<sup>99</sup> Data collected from secondary sources is compared to the content delivered by interviews and combined to a whole picture of understanding.

## Expert Interviews and Guideline

Open guided interviews are used for verbal data collection to obtain factual statements in close proximity to the specific subject.<sup>100</sup> They offer insights into structural relations and procedures of specific systems and enable interpretations based on experiences.<sup>101</sup>

---

<sup>93</sup> Mazarr, M.J. 2020.

<sup>94</sup> Hamilton, D.S. 2010.

<sup>95</sup> Helfferich, C. 2019; Bogner, A. et al. 2014.

<sup>96</sup> Raediker, S. and Kuckartz, U. 2019; Kuckartz, U. 2018.

<sup>97</sup> Mayring, P. 2000.

<sup>98</sup> Miles, M.B. and Huberman, A.M. 1994; Creswell, J.W. 2014.

<sup>99</sup> Blaikie, N.W.H. 1991, p. 116; Eisenhardt, K.M. 1989, pp. 537 et seq.; Andresen F. 2017, p. 118; Ruona, W.E.A. 2005, p. 248; Creswell, J.W., p. 234; Yin, R.K. 1992, p. 131.

<sup>100</sup> Mayer, H.O. 2013, p. 37; Helfferich, C. 2019, pp. 669, 680 et seq.; Miles, M.B. and Huberman, A.M. 1994, p. 10; Bogner, A. et al. 2014, p. 3.

<sup>101</sup> Liebold, R. and Trinczek, R. 2009, p. 53.

In this case, expert interviews seemed appropriate and necessary since the topic requires NATO internal knowledge and experience of processes and structures.<sup>102</sup> However, expert interviews also have the difficulty and widely discussed function of how to derive a generalization of collected data and how to enable a transfer of that knowledge to other areas.<sup>103</sup> In this study, generalizability is not sought. The focus is less on the sample size (in the meaning of saturation) itself but more on the adequacy of the experts.<sup>104</sup> With “particularity rather than generalizability is the hallmark of good qualitative research”, this study follows Creswell.<sup>105</sup>

The characteristic of this type of interview with a standardized guideline is the open formulation of questions and the consistency of the guideline,<sup>106</sup> which prevents drifting off into less essential topics in a fluent conversation. However, a strict order should be neglected, as otherwise, the course of the conversation and the answers could be severely restricted.<sup>107</sup> Therefore, open interviews only refocus or redirect the conversation in case of missing the intention of the interview. Following the advice of Miles and Huberman regarding a ‘good qualitative researcher-as-instrument’, theoretical and content-related knowledge of NATO and resilience has been gained in order to conduct relatively reliable and valid interviews.<sup>108</sup>

The design of the guideline is based on the scientific principles of social research and symbolizes the structure of themes and topics along with being a helpful tool for the collection of data.<sup>109</sup> In order to be able to conduct a guided interview with experts for answering the research question, a clear concept and understandable questions are required.<sup>110</sup> Based on the construct of the term, nominal definition, and operationalization,<sup>111</sup> a guideline was designed, which included categories based on the principles of Höpflinger.<sup>112</sup> All modules started with a question that is formulated as open as possible. For answering the research question, it was essential to know more about the opinion of the participants with regard to definitions and the specific role of NATO. Based on this understanding, it was interesting to know

<sup>102</sup> Mayer, H.O. 2013, p. 37; Liebold, R. and Trinczek, R. 2009, pp. 33 et seq.; Creswell, J.W. et al. 2007, pp. 247 et seq.; Bogner, A. et al. 2014, pp.

<sup>103</sup> Mayer, H.O. 2013, p. 39; Flick, U. 2011, S. 108; Miles, M.B. and Huberman, A.M. 1994, p. 1.

<sup>104</sup> O’Reilly, M. and Parker, N. 2012, p. 192

<sup>105</sup> Creswell, J.W. 2014, p. 253.

<sup>106</sup> Helfferich, C. 2019, pp. 670, 682; Bogner, A. et al. 2014, p. 24; Liebold, R. and Trinczek, R. 2009, pp. 33, 38.

<sup>107</sup> Mayer, H.O. 2013, p. 37; Gioia, D.A. et al. 2012, p. 20; Bogner, A. et al. 2014, p. 28. <sup>50</sup> Andresen, F. 2017, p. 119

<sup>108</sup> Miles, M.B. and Huberman, A.M. 1994, p. 38; Creswell, J.W. 2014, p. 234; Rieker, P. and Seipel, C. 2006, p. 4039; Liebold, R. and Trinczek, R. 2009, pp. 38 et seq.

<sup>109</sup> Bogner, A. et al. 2014, pp. 27 et seq.; Liebold, R. and Trinczek, R. 2009, p. 35.

<sup>110</sup> Helfferich, C. 2019, pp. 669 et seq.; Liebold, R. and Trinczek, R. 2009, p. 38.

<sup>111</sup> Mayer, H.O. 2013, pp. 11 et seq.; Helfferich, C. 2019, pp. 670 et seq.; Miles, M.B. and Huberman, A.M. 1994, p. 58.

<sup>112</sup> [https://www.uibk.ac.at/iez/mitarbeiterinnen/senior-lecturer/bernd\\_lederer/downloads/praktische-regeln-zur-formulierung-von-fragen-fuerfragebogen.pdf](https://www.uibk.ac.at/iez/mitarbeiterinnen/senior-lecturer/bernd_lederer/downloads/praktische-regeln-zur-formulierung-von-fragen-fuerfragebogen.pdf)



Category	Theme	Guideline Questions
Definition	1 Resilience Definition	How would you define resilience in your field of expertise?
	Bounce Back Definition	What do you think of NATO's "Bounce back Resilience" definition?
	2 Societal Resilience Definition	How would you define societal resilience?
NATO's role	3 NATO's Role in Strengthening Societal Resilience	What role might/should NATO play in strengthening the societal resilience of member states?
	4 8th Baseline Requirement	Take into consideration that NATO BRs are reviewed currently especially in the light of the societal resilience perspective. Do the NATO BR requirements need a new "8th" requirement to specifically include the strengthening of the societal resilience?
	Challenges/Obstacles of NATO Societal Resilience	What challenges/obstacles for NATO do you see in strengthening the societal resilience of NATO member states?
	5 East-West Divide	From a NATO/Academic/National government official point of view, are there reservations within the nations regarding the strengthening of societal resilience due to the different threat perceptions (e.g. East-West divide)?
	NATO Civilian Sector Engagement	Given that resilience must be addressed primarily in the civilian sector and is first and foremost a national responsibility, do nations really want NATO to engage in this field?
	6 COVID-19 Lessons Learned	What opportunities/lessons learned do you see in strengthening the societal resilience of NATO member states in the aftermath of the COVID-19 pandemic?
Policy	7 Concrete Measures & Capabilities	How can NATO concretely strengthen the societal resilience of its member states? Which measures? Which capabilities?
	4th Core Task	What do you think about the idea of integrating resilience into NATO's new strategic concept as a fourth core task in order to enhance resilience?
Development	8 Resilient Society from Scratch	If you could create a resilient society "from scratch", what would be its core elements?
Reflection	9 CIMIC and CMI Contribution	In the case of a NATO operation (collective defense, cooperative security, crisis management), what could be the contribution of CIMIC and CMI to improve societal resilience, or is there any part or specific element that CIMIC and CMI could provide in this area?

Fig. 2 Categorized questions for expert interviews. (Own illustration)

how they see resilience coming into place, what kind of challenges and possibilities the participants see, and what kind of influence the pandemic situation was having. Another approach was to ask the participants for a description of a perfect resilient society and how the role of CIMIC fits into NATO's policy. Formulated as open questions, the entire guideline offered sufficient options for the interviewed experts to introduce and refer to other relevant aspects.

For structuring the guideline, the questions have been categorized inductively into themes and finally into categories. That creates a primary structure and supports the coding of the interview data in the final step.<sup>113</sup>

Applying a pretest gives the opportunity to refine the questions and underlines the importance of the expert interview.<sup>114</sup> The pretest took place as an expert review.<sup>115</sup> This offered the opportunity to adapt questions that had been too complex and formulated incomprehensibly.<sup>116</sup> After the preliminary conceptual design of the desired expert groups and the scientifically sound development of a final guideline, 11 experts were interviewed virtually (video conference platform WebEx) (Fig. 2).

### Sample Size and Choice of Experts

The large number of experts for "Resilience" in NATO and the academic world asked for a selection of samples or representatives in advance.<sup>117</sup> The key function

<sup>113</sup> Liebold, R. and Trinczek, R. 2009, pp. 37 et seq..

<sup>114</sup> Helfferich, C. 2019, p. 682; Bogner, A. et al. 2014, p. 34.

<sup>115</sup> Lenzner, T. et al. 2016, p. 2.

<sup>116</sup> Mayer, H.O. 2013, p. 45; Lenzner, T. et al. 2016, p. 1.

<sup>117</sup> Mayer, H.O. 2013, pp. 38 et seq.; Almaki, S. 2016, p. 289; O'Reilly, M. and Parker, N. 2012, p. 193; Bogner, A. et al. 2014, p. 34.

of such samples in data collection is constituted differently, as quantitative research methods focus on statistical representativeness.<sup>118</sup> Specific criteria are defined in advance and used to select particular experts. The requirements depend on the research question and other theoretical considerations, which are also applied to this study.<sup>119</sup> The main criterion was working in or for NATO, especially in a resilience-related area, so the participants can provide more in-depth information on policy and identify problems and challenges as well as recommendations for action.<sup>120</sup> This means experts from a political, strategic, and operational level, as well as academic field, were necessary in order to answer the research question comprehensively.<sup>121</sup> The choice of experts has been made deductively. The experts answered the questions openly but structured topic-wise, which means that those interviews can be interpreted inductively. Thus, the inductive and deductive procedure and characteristics of the expert interview go hand in hand.<sup>122</sup> Due to known academic experts by publications and references in literature and existing relations to NATO HQ (Brussels) and SHAPE (Mons), potential experts were identified and categorized as follows:

- Four Subject Matter Experts from NATO (NATO Headquarters, Supreme Headquarters Allied Powers Europe (SHAPE), Joint Force Command Brunssum, JFCBS, CIMIC Centre of Excellence (CCOE) – category N (NATO)
- Three Subject Matter Experts from NATO member states working in the Civil Emergency Planning Committee (CEPC) – category M (member states)
- Four Subject Matter Experts from Universities or Think Tanks – category A (academia)

Experts from the first group “NATO” are referred to as N, M stands for the second group “Member States”, and A for the last group “Academia”.

The explorative part of this research required an extended sampling in order to elaborate on a broad spectrum of positions, challenges, ideas, and solutions. The interviews with representatives from these three different groups took those considerations into account.<sup>123</sup> As it is not the aim of qualitative research to acquire a fixed number of participants, this research focuses on the sufficient depth of specific information.<sup>124</sup> In this respect, the appropriateness and adequacy of the sampling are the two key drivers. This sample size was rated to deliver valuable insight and sufficient opinions to interpret and answer the research question. As O’Reilly and Parker state “there will always be new things to discover” and, therefore, “data are

<sup>118</sup> Mayer, H.O. 2013, p. 39; O’Reilly, M. and Parker, N. 2012, p. 192.

<sup>119</sup> Mayer, H.O. 2013, p. 40; Bogner, A. et al. 2014, p. 35.

<sup>120</sup> Miles, M.B. and Huberman, A.M. 1994, p. 27.

<sup>121</sup> Gläser, J. and Laudel, G. 2009, pp. 11 et seq.

<sup>122</sup> Liebold, R. and Trinczek, R. 2009, p. 37.

<sup>123</sup> Bogner, A. et al. 2014, pp. 34 et seq.; Creswell, J.W. 2014, p. 239.

<sup>124</sup> O’Reilly, M. and Parker, N. 2012, p. 195; Creswell, J.W. 2014, p. 239; Gioia, D.A. et al. 2012, p. 16.

never truly saturated”.<sup>125</sup> Nevertheless, saturation has been achieved within the pre-set restrictions of this work by applying adequate preliminary literature viewing in combination with the expert interviews.

The experts were contacted by e-mail and the online platform LinkedIn. Consequently, 11 open interviews were conducted in the timeframe of 7 months online as COVID-19 restrictions excluded other options. The interviews lasted 30–45 min. They were audio- and video-recorded and transcribed afterwards verbatim. Every participant had agreed to the recording in advance.<sup>126</sup> The interviews were not executed anonymously but anonymised afterwards for the findings section of this study. That way, the final interpretations and opinions are presented for each group instead of a single person. During the interviews, notes were taken and added to the protocol of each interview.<sup>127</sup>

### 5.3 *Data Analysing and Evaluation and Interpretation*

A core but least formally structured part is analysing the collected data.<sup>128</sup> The variety of sources asks for some structures nevertheless. According to Ruona this process entails sensing themes, constant comparison, recursiveness, inductive and deductive thinking, and interpretation to generate meaning.<sup>129</sup> Collecting and analysing data is a simultaneous process<sup>130</sup> as first analytical thinking enables adaptation and adjustment of the collection process. Same applies to analysing and evaluating. So these three phases should be seen in a feedback loop rather than in a strictly linear timeline,<sup>131</sup> although too much analysis and evaluation at a too early stage might lead to interference and influence on the data collection, for example, by a reduction of collected data by focussing the interview based on premature conclusions. The evaluation of this study focused on the interpretive approach,<sup>132</sup> especially on words as the basic form of data, in which the central task is not only to code but to question and classify what has exactly been said in the interviews.<sup>133</sup>

---

<sup>125</sup> O’Reilly, M. and Parker, N. 2012, p. 192 et seq.

<sup>126</sup> Bogner, A. et al. 2014, p. 40.

<sup>127</sup> Creswell, J.W. 2014, p. 244; Gioia, D.A. et al. 2012, p. 19; Bogner, A. et al. 2014, pp. 39 et seq.

<sup>128</sup> Eisenhardt, K.M. 1989, p. 539.

<sup>129</sup> Ruona, W.E.A. 2005, p. 236.

<sup>130</sup> Creswell, J.W. 2014, p. 258; Gioia, D.A. et al. 2012, p. 20; Glaser, B.G. and Strauss, A.L. 1967, p. 364.

<sup>131</sup> Andresen, F. 2017, p. 120; Miles, M.B. and Huberman, A.M. 1994, pp. 10 et seq.; Creswell, J.W. 2014, p. 245; Glaser, B.G. and Strauss, A.L. 1967, p. 364.

<sup>132</sup> Bogner, A. et al. 2014, p. 72.

<sup>133</sup> Mayer, H.O. 2013, p. 25.

Data management is a necessary step and marker of quality referring to the transparency of the research and systematically collecting of new data.<sup>134</sup> The collected interview data were evaluated by using MAXQDA, a software for computer-assisted qualitative data, and text analysis.<sup>135</sup> The qualitative audio and visual materials were saved as MP4 files (video) and M4A files (audio).<sup>136</sup> By using the software “Amberscript”, the data were transcribed verbatim, applying generalized transcription rules by Kuckartz<sup>137</sup> into a Microsoft Word (Docx) file.<sup>138</sup> Clustering pieces of collected data into individually identified categories for providing a better understanding of the context is the main purpose of those systems in general.<sup>139</sup> That can be done inductively or deductively.<sup>140</sup> According to Kuckartz this is called “Coding” (discovering and conceptualizing)<sup>86</sup> and means in this study interpreting information topic-wise in category-based qualitative content analysis.<sup>141</sup> Deductive coding means building categories before going through the collected data (concept-driven).<sup>142</sup> The data get classified into those different categories (“tagging”).<sup>143</sup> In this sense, achieving saturation becomes unrealistic as categories that may emerge from data will not be recognized.<sup>144</sup> Inductive coding in contrast means realizing categories after analysing the collected data and is often constructed as a hierarchical system iteratively (data-driven).<sup>145</sup> It is an active iterative process that refines itself with every iteration of coding.<sup>92</sup> In this case, data can be saturated due to the focused idea that guides the direction of collecting data.<sup>146</sup>

<sup>134</sup> Miles, M.B. and Huberman, A.M. 1994, p. 45; O’Reilly, M. and Parker, N. 2012, p. 193.

<sup>135</sup> Flick, U. 2011, p. 104; Ruona, W.E.A. 2005, pp. 250 et seq.; Creswell, J.W. 2014, p. 245; Bogner, A. et al. 2014, pp. 83 et seq.; Liebold, R. and Trinczek, R. 2009, p. 43.

<sup>136</sup> Creswell, J.W. 2014, p. 240.

<sup>137</sup> Raediker, S. and Kuckartz, U. 2019, p. 44.

<sup>138</sup> Raediker, S. and Kuckartz, U. 2019, pp. 3 et seq.; Miles, M.B. and Huberman, A.M. 1994, p. 51; Liebold, R. and Trinczek, R. 2009, p. 41.

<sup>139</sup> Mayring, P., 2000, p. 3; Miles, M.B. and Huberman, A.M. 1994, pp. 44 et seq.; Raediker, S. and Kuckartz, U. 2019, p. 5.

<sup>140</sup> Miles, M.B. and Huberman, A.M. 1994, p. 63; O’Reilly, M. and Parker, N. 2012, p. 194; Ruona, W.E.A. 2005, p. 238; Creswell, J.W. 2014, p. 234. <sup>86</sup> Ruona, W.E.A. 2005, p. 241.

<sup>141</sup> Raediker, S. and Kuckartz, U. 2019, p. 4; Kuckartz, U. 2018, pp. 97–117.

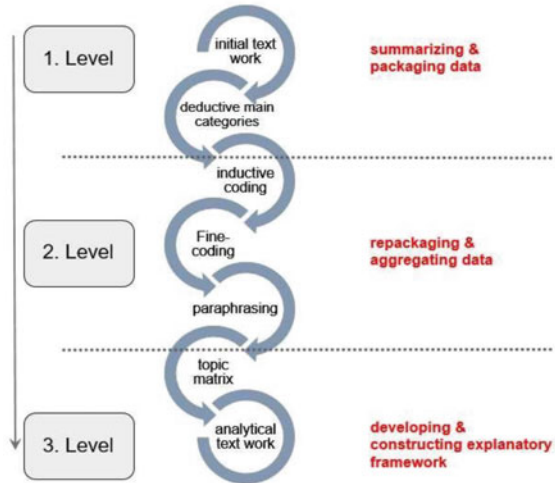
<sup>142</sup> Raediker, S. and Kuckartz, U. 2019, p. 98; O’Reilly, M. and Parker, N. 2012, p. 194; Ruona, W.E.A. 2005, p. 238.

<sup>143</sup> Raediker, S. and Kuckartz, U. 2019, p. 69; Ruona, W.E.A. 2005, p. 241.

<sup>144</sup> O’Reilly, M. and Parker, N. 2012, p. 194.

<sup>145</sup> Raediker, S. and Kuckartz, U. 2019, p. 98; Miles, M.B. and Huberman, A.M. 1994, p. 58; O’Reilly, M. and Parker, N. 2012, p. 194; Ruona, W.E.A. 2005, p. 238; Rieker, P. and Seipel, C. 2006, p. 4039. <sup>92</sup> Raediker, S. and Kuckartz, U. 2019, p. 102.

<sup>146</sup> O’Reilly, M. and Parker, N. 2012, p. 194.



**Fig. 3** Phases of qualitative content analysis, inspired by Kuckartz, Miles, and Huberman. (Own illustration)

Following the content-structuring analysis, the interviews were analysed, evaluated, and structured in seven different phases.<sup>147</sup> This procedure is based on the original content analysis of Mayring.<sup>148</sup> That specifically means that all individual categories have been coded from the data material (“inductive”) as well as from the research question and interview guide (“deductive”).<sup>149</sup> Therefore, saturation and adequacy of content could be achieved. Influenced by Carney and Miles and Huberman,<sup>150</sup> the seven phases of Kuckartz are displayed in the following way (Fig. 3):

The first phase represents the initial text work, in order to get familiar with the data material. In the second phase, thematic main categories were deductively derived based on the modules of the interview guide. In the third phase, new subcategories are coded and generated inductively. It is important to know that having too many subcategories leads to a higher risk of failure in coding. The fourth phase focuses on reviewing, revising, and fine-coding of all deductive-inductive coding.<sup>151</sup> This includes seeking similarities and differences among those categories.<sup>152</sup> Phases 5 and 6 symbolize the paraphrasing and creation of the topic matrix, and, finally, the last phase consists of the actual analytical text work of

<sup>147</sup> Kuckartz, U. 2018, p. 100.

<sup>148</sup> Mayring, P. 1994, p. 164.

<sup>149</sup> Bogner, A. et al. 2014, p. 74; Miles, M.B. and Huberman, A.M. 1994, p. 17.

<sup>150</sup> Miles, M.B. and Huberman, A.M. 1994, p. 92.

<sup>151</sup> Kuckartz, U. 2018, p. 97 et seq.

<sup>152</sup> Gioia, D.A. et al. 2012, p. 20.

Aggregate Dimensions		2nd Order Themes / Deductive (1. Level)	Inductive (2. Level)
Definition	1	Resilience Definition	Legal Foundation Core Elements Resilience Stakeholders Threats Criticism of Definition
		Bounce Back Definition	Agree Disagree
	2	Societal Resilience Definition	Same Definition as Resilience New Perspective in Security Policy Goals of Societal Resilience Building Blocks of Societal Resilience
NATO's role	3	NATO's Role in Strengthening Societal Resilience	Cooperation with EU National Responsibility - Collective Commitment - NATO Support NATO should enhance Resilience of Democracy
	4	8th Baseline Requirement	Agree Disagree
	5	Challenges/Obstacles of NATO Societal Resilience	Operational Issues Society's Culture Political Culture of NATO Allies
		East-West Divide	Factors for Enhancing Societal Resilience Policies
	6	NATO Civilian Sector Engagement	National Responsibility - Collective Commitment
Policy	7	Concrete Measures & Capabilities	Cascading Effects Civil Preparedness Political Framework Hybrid Activities NATO's Role Resilience Goals Means to Achieve the Goals EU - NATO Cooperation
		4th Core Task	Agree Disagree Not Sure
Development	8	Resilient Society from Scratch	Education Policy Democracy
Reflection	9	CIMIC and CMI Contribution	Supportive Role Liaison Awareness of Civil Situation

Fig. 4 Coding categories. (MAXQDA – own illustration)

the data material.<sup>153</sup> Paraphrasing in this context is an inductively summarized expression of specific content.<sup>154</sup>

In that way, the content could be presented in subcategories, based on transcribed interviews.<sup>155</sup> This coding process is an ongoing process that might uncover sources of bias<sup>156</sup> and gives the opportunity to react and improve the next interview. Categories have to be defined accurately. That way those categories are explicitly distinguishable from each other and function as an analytical framework and coding guideline.<sup>157</sup> According to Ruona, the categories should reflect the purpose of the research, be exhaustive, mutually exclusive, sensitizing, and conceptually congruent (Fig. 4).<sup>158</sup>

As Miles and Huberman state “the structure, as revised, will include codes that are ‘larger’ [...] and ‘smaller’ [...], but it will need to maintain a relational structure”. This relational structure is shown in the created subcategories above, which have been built inductively. The first-level code is a single term that can

<sup>153</sup> Kuckartz, U. 2018, p. 97.

<sup>154</sup> Raediker, S. and Kuckartz, U. 2019, pp. 144, 147.

<sup>155</sup> Mayer, H.O. 2013, p. 45; Ruona, W.E.A. 2005, p. 241.

<sup>156</sup> Miles, M.B. and Huberman, A.M. 1994, p. 65.

<sup>157</sup> Raediker, S. and Kuckartz, U. 2019, pp. 100 et seq.

<sup>158</sup> Ruona, W.E.A. 2005, pp. 242 et seq.

be differently interpreted by authors easily. Beginning with definitions and more generic knowledge about NATO and resilience in general, the guideline focused more on societal resilience and measures after the door opener “pandemic situation”. Deductively 13 categories were developed on the first level. Taking all information from interviews and documents into account, the above-listed subcategories were inductively evolved on the second level. The second-level coding (pattern coding) consists of themes and constructs that describe the first-level code. That way it is easier to analyse during data collection and the researcher gets more focused on future interviews.<sup>159</sup> The third level, meaning the analytical work, is the discussion and interpretations from those previous levels.

## 5.4 *Timeframe*

The study and the interviews were conducted within a 7-month timeframe from March to October 2021. Not all statements reflect the developments in Ukraine since February or the results of the NATO summit in Madrid in June 2022.

Some of the recommendations of the study, such as the development of a layered resilience concept, are already reflected in others, such as establishing Resilience as the fourth core task of the Alliance did not materialize.

For further research, it is interesting to find out more perspectives and different actors in that area and compare those opinions to the ones already known and finally get closer to the point “when the incremental improvement to theory is minimal”.<sup>160</sup> There were also limitations in getting necessary documents regarding NATO and basic theory. Due to the research question itself and various questions of the guideline, a potential bias could have occurred. In applying triangulated data, the bias has eventually been overcome. In this type of study, it is essential to mention that there can be no unambiguous interpretation of the results, and therefore there is always room for other opinions, inevitably.<sup>161</sup>

## 6 Results

In the following section, the results of the explorative research are presented. The order is based on the modules of the interview guideline.

---

<sup>159</sup> Miles, M.B. and Huberman, A.M. 1994, pp. 62 et seq

<sup>160</sup> Eisenhardt, K.M. 1989, p. 545.

<sup>161</sup> Mayer, H.O. 2013, p. 47.

## 6.1 *Module 1: Definition*

### **Resilience Definition**

Two NATO representatives (N) noted that there is no agreed official definition, which leads to problems in operationalization. On the other hand, a representative of the member states (M) explained that because resilience is such a broad concept, a legally binding definition would severely limit the Alliance's room for manoeuvre with regard to the challenges in this area. Rather, it is sufficient that a common understanding of what resilience means is currently found in order to implement this in the best possible way with the help of RtCP. The majority stated that the basis for NATO's entire resilience policy is Article 3 of the Washington Treaty (7 from N, M, and A). One M additionally stated that the fulfilment of the third article is the cornerstone for the implementation of the fifth article. N participants declared that the Crimea annexation following analysis of member states' civil preparedness capabilities led to the Alliance's resilience Commitment at the NATO Summit in Warsaw in 2016. Therefore, resilience is actually the first line of defence and describes its deterrent role on potential attackers. According to N officials "Resilience through Civil Preparedness" is notified as NATO language and should always be mentioned in connection with NATO's resilience policy (3 N).

Seven out of 11 (N, M, A) described resilience as the ability of a state to withstand a strategic shock (regardless of its nature) and emerge stronger: three went into detail and stated that it is elementary to adapt to those effects in order to be better prepared for similar events in the future. Two N officials further explain the fundamental role of RtCP as it enables countries to better protect their population and ensures efficiently acting military forces within the framework of a NATO operation. One A pointed out the necessity of knowing the possible threat for implementing effective countermeasures.

Only one N described all the mentioned core stakeholders in NATO's resilience policy.

Six participants (N, M, A) agreed that RtCP is directed against the entire spectrum of threats (armed conflicts, natural disasters, man-made disasters, hybrid attacks, terrorism, and global phenomena such as pandemics or climate change). Two interviewees (A) pointed out that it is irrelevant whether the threat comes from state or non-state actors.

According to four members from M and A, RtCP is a very broad and not concrete concept. One A also noted that the working definitions of resilience are very simplified. Another A criticized that RtCP only centres on the members of the Alliance and should be externalized and expanded to support partner and neighbouring nations.

Interpreting conclusions resilience as the "first line of defence" represents the ability of a state in the alliance to withstand an external or internal shock (against the "full spectrum of threats"),<sup>162</sup> to recover from it as quickly as possible, and then

---

<sup>162</sup> Ruehle, M. and Roberts, C. 2021, p. 4.



to undergo an adaptation process aimed at making the state structures more resilient based on the experience gained.

The research showed that although there is no officially agreed NATO definition, there seems to be a general understanding of what resilience means in the Alliance context. The fact that there is no official definition of resilience leaves room for interpretation and by that provides flexibility for nations but at the same time misses to set standards for the implementation.

### **“Bounce-Back” Definition**

Six of the interviewees (N, M, A) were positive about NATO’s view of the “bounce-back” effect. One respondent (N) further claimed that this term was taken from general scientific resilience research. One M, in particular, agreed that it was the process after a strategic shock or crisis in which state structures, the economy, as well as a society evolve in order to be adequately prepared for future, similar, or related challenges.

With one exception, all A rejected the NATO “bounce-back” perspective. Three argued that it was a very simplified representation of many complex individual processes, which did not take place in a jerky manner in the literal sense of “bounce-back”, but rather resembled a long-term adaptation process. Furthermore, the term implies a desire to return to the precrisis state, which should not be the goal. Instead, a better-prepared state is focused as the suggested term “bounce-forward” indicates.

Finally, in the context of describing NATO’s resilience, the term “bounce-back” effect is often used. This term is viewed critically, especially by scientists. Nevertheless, the term should be retained in the context of the striking simplification of a complex issue in order to ensure coherent communication both externally and internally. However, it should be made clear that this is not so much a rapid, literal “bounce-back” process but rather a long-term, forward-looking adaptation process.

### **Societal Resilience Definition**

Ten participants (N, M, A) stated that societal resilience would mean the same thing to them as it does for resilience. Only that in this case it referred primarily to the resilience of the third stakeholder: the civil society, the citizens, and the community. Six members (N, M, A) noted that societal resilience is a very broad and complex concept, which needs an elaborate understanding of one’s own society first. The question of who are the addressees of activities/measures to increase societal resilience needs to be clarified as well.

Since the increasing emergence of hybrid and cyber campaigns aimed at directly influencing and ultimately harming societies of NATO countries and the impact of the COVID-19 pandemic, there has been a shift in perspective regarding societal resilience, as one N framed these changes historically.

According to one person (N), the new NATO initiative to promote societal resilience primarily pursues three goals: first, the countries of the alliance should train their citizens to become so-called first responders light and thus support the

“real” first responders (public emergency services, fire brigade, police, emergency services, etc.) in major emergencies. The background to these considerations is that civilians would usually be at the scene of the damage before the emergency services and could help immediately if they were appropriately trained.

The second focus of NATO’s efforts is the fight against misinformation and disinformation, based primarily on the experience of the COVID-19 pandemic. The massive impact of the hybrid campaigns made it clear that further preventive and countermeasures need to be developed and implemented. The third goal was to involve citizens more closely in national defence efforts, one NATO representative explained. This primarily involved the development of “best practices” based on the experiences of the “Total or Comprehensive Defence Model” of the Scandinavian countries. However, this is a politically sensitive issue for some NATO countries due to cultural reservations about the formal involvement of citizens in national security strategies.

Two N further noted that societal resilience involves several levels. These are the strategic, regional, local, and individual levels. They also noted that NATO had a maximum influence on the strategic level within the framework of national competence in this area. In this context, one interviewee (A) operationalized societal resilience using the mentioned model according to Versteegden.<sup>163</sup>

A high level of trust (of society) in the state structures, the political system, and the executive was considered by seven of the respondents to be the most important building block of societal resilience. Complementing this, two N explained that in addition to trust in the government apparatus, there must be a common threat perception and the will of the people to manage this threat together (cohesion).

Summarizing the interview study, societal resilience is seen as the resilience of the third stakeholder, society. This means that society must be able to withstand threats, whether internal or external, recover quickly from strategic shocks and crises, and then adapt. Based on the data analysis, two essential characteristics of a resilient society could be identified, which, however, have to be considered in an interdependent and multidimensional way. These are the characteristics: “democracy and trust” and “informed and resilient citizens”.

An elementary prerequisite for a resilient society is a functioning democratic system, with strong institutions and clear, shared norms and values. These include, but are not limited to, openness, transparency, rule of law, and good governance. An inclusive, democratic society is the first step towards a resilient nation. In this context, a high level of societal trust in state institutions and in the legitimacy of the government is another important basic condition of societal resilience. Only if citizens understand the measures taken against a crisis or strategic shock and can see the meaning and purpose behind these measures will they follow the rules despite both personal and societal costs and at the same time be less vulnerable to negative external influences. The second pillar of a resilient society is its citizens. They need to be empowered to the extent that they are considered well-informed,

---

<sup>163</sup> Versteegden, C. 2018, pp. 25 et seq.

resilient citizens. This should enable a paradigm shift in the relationship between the state and citizens in the event of a crisis or disaster. Citizens should no longer only be passive, vulnerable individuals in need of protection but should be empowered to support national security preparedness as active contributors. To this end, information material can be developed and distributed to every household. This promotes individual resilience, which also includes, for example, stockpiling emergency supplies. Likewise, resilience courses can be offered to children, youth, and adults, the completion of which can be incentivized (e.g. credits for universities and tax breaks for adults). The knowledge and training gained by the citizens should be regularly trained with exercises. In addition, an informed and resilient society should have sufficient media literacy to deal with mis- and disinformation. On the one hand, this means that people of all social and age groups must be trained accordingly, in kindergarten, school, adult education centres, and public institutions. On the other hand, it also means that the state must be able to provide citizens with accurate and transparent information quickly, which leads to a dilemma between freedom of the information environment and restrictions.

## ***6.2 Module 2: NATO's Role***

### **NATO's Role in Strengthening Societal Resilience**

Ten of the respondents (N, M, A) agreed that promoting resilience is first and foremost a national competence and accordingly that member states have the leading role. NATO's role is primarily supportive or coordinative. One N clarified that the role is strictly limited to the strategic-national level. The operationalization is the responsibility of the states themselves within the scope of their possibilities. One interviewee (A) explicitly pointed out that this was a mostly civil matter and therefore no "securitization" of the issue should be undertaken.

Furthermore, seven respondents (N, M, A) explained that NATO should support the promotion of resilience within the scope of its possibilities (via the CEPC (new name since MADRID Summit) and its planning groups). This includes the development of a framework but above all the provision of a platform for the exchange of experiences, ideas, opinions, general information, and the establishment and maintenance of a "best practice toolkit" for the Alliance. Two of these participants (N) pointed out that it is possible for the CEPC in particular, to assemble a resilience advisory team from the pool of experts. The team supports the requesting nation's national structures.

From one A's point of view, NATO's role is much broader and needs a mechanism to promote democracy and Western values to be added to the resilience policy as countries that do not sufficiently protect their democracy and values are more vulnerable to potentially disruptive developments. That points out a dilemma between the alliance cohesion and national interests.

Interpreting these results it should be noted that promoting resilience is first and foremost a national responsibility. Although resilience also has collective implications and must therefore be thought of within the NATO framework, NATO's role is primarily coordinative and supportive. The member states take on a far more important role, which reveals the dilemma between national responsibility and erosion of state powers.

The CEPC is to continue to support the member states by further developing the RtCP framework, producing guidelines, and providing a platform for discussion, pooling capabilities and resources, and exchange. Furthermore, "best practice" recommendations are to be developed.

### **8th Baseline Requirement**

Three A called for NATO to develop an eighth, new BLR to promote societal resilience. In addition, two further stated the importance of the involvement of society in decision-making processes related to societal resilience, in line with a "whole of society approach". Another A noted that the BLRs clearly focus on the protection of critical infrastructure. In addition, a new BLR should therefore place more emphasis on the perspective of societal resilience.

Seven respondents (N, M, A) said that the BLRs do not need any changes. Further, interviewees commented that promoting societal resilience carries multidimensional and cross-cutting implications across all BLRs. Therefore, they suggested that each BLR should be supplemented with regard to the inclusion of aspects of societal resilience. One A even flatly rejected RtCP and thus BLRs as it is not the right approach to deal with these challenges for the Alliance in this area.

Two N suggested that the seven BLRs are a widely accepted and known concept. Changing this could cause confusion and pose a challenge for the strategic communication of the concept both externally and internally. One N explained that societal resilience is not the end state but just another mean to achieve the goal of a resilient state. Therefore, the BLRs were developed in an overarching way and not specifically tailored to one stakeholder. Another participant (A) criticized that the BLRs follow a "top-down approach" and are therefore too inflexible.

Finally, the survey shows that the majority of respondents do not consider it sensible to enhance societal resilience by adapting the BLRs and thus creating an eighth BLR. There are some voices that contradict this opinion but mainly with the argument that a new eighth BLR will increase the political pressure to act in this field. This view cannot be followed for several reasons. Societal resilience is a multidimensional and cross-cutting issue that has implications for all BLRs. Therefore, all BLRs should be reviewed by the CEPC for these implications and adapted accordingly to adequately address societal resilience.

Furthermore, it should be noted that it would be analytically questionable to assign a separate requirement to societal resilience. Since the BLRs are primarily sector- or cross-sector-focused and not stakeholder-centred. Based on these mea-

asures, societal resilience would be given the prominent status that this field deserves even without the development of a new BLR.

### **Challenges/Obstacles of NATO's Societal Resilience**

Eight of the interviewees (N, M, A) saw the greatest challenge above all in the fact that the promotion of resilience and thus also societal resilience falls primarily within the sphere of competence of the member states and that NATO's role is therefore only of a supporting nature. Thus, the further development of the resilience policy depends on the political will of the Alliance nations. Two A emphasized that societal resilience is primarily a civilian challenge and that military capabilities and capacities are important but should not come first.

One N and one A saw one of the main challenges at the operational level of societal resilience as being how this could be measured across the Alliance. Due to the divergent cultural, social, media, economic, and political composition of the societies of the NATO countries, it is very difficult to develop overarching, comparable indicators in this area. In addition, there is the question of how to reliably measure supposedly intangible indicators such as "trust in the government and its institutions".

Six participants (N, M, A) also stated that they saw a challenge in defining society. For example, it would first have to be clarified what exactly society consisted of. It would hardly be possible to involve every single citizen in the decision-making process in the context of developing measures to promote societal resilience. Therefore, it is necessary to address selected groups, but this carries the risk that the state cannot maintain the required inclusiveness and representativeness of its citizens.

Two M and one N classified the different national political-legal frameworks in the implementation of measures to promote societal resilience in the Alliance as further major challenges. For example, the rather centralized political system in the Netherlands differs greatly from the federal system in Germany. In Germany, more stakeholders need to be considered, which makes the decision-making process more complex. "This shows that each member state has a unique constitutional system, social contracts, and stakeholders. This is a major challenge to reach a political agreement", the NATO official said.

Two N stated that another problem is that NATO member states are very reluctant to share the current state or capabilities of their civil defence structures with their allies through the State of the Civil Preparedness Report (or other formats). This is a non-mandatory questionnaire designed by CEPC. Thus, no particular needs or challenges could be identified in order to develop any specific measures. This is mainly due to national pride and national security concerns of some member states, according to N. One A stated that in order to be able to improve the area of early warning systems of threats, the integration of more qualitative and quantitative data (especially data science and big data) is necessary as a large number of organizations

and authorities are active, which leads to competence diffusion and confusion. He, therefore, proposed streamlining the structures and a clear process owner.

For giving an interpreted summary, the main challenge is that, as explained in the previous research question, NATO is not the main stakeholder in the field of (societal) resilience. While member states have agreed to strengthen their resilience through the Washington Treaty, the 2016 Resilience Commitment, and the 2021 Resilience Commitment, all three documents are legally nonbinding commitments. This means that the extent to which societal resilience is strengthened ultimately depends on the political will of the Alliance members.

It can be assumed that other mainly political challenges, such as the diverging threat perceptions and the different historical and cultural perspectives as well as political systems of the countries in the alliance, will have an influence on the future of NATO's societal resilience. Due to their geographical proximity to a potential aggressor but also due to their historical experiences, the Northern and Eastern European NATO countries have a much more positive attitude towards strengthening societal resilience than the Southern and Western European Allies. This is mainly due to the fact that most citizens of these states have only a limited interest in matters of national security or fear a militarization of society and therefore reject societal resilience. However, this is primarily a cultural problem. Nevertheless, it is therefore important to convey that the creation of societal resilience does not mean militarization but rather the creation of redundancies. Furthermore, cross-cutting areas of interest must be identified in joint exchange and dialogue. Based on this, measures and concepts must be developed that all states in the Alliance can support.

A final challenge that needs to be discussed mainly at the member state level, but is also relevant to NATO's RtCP framework, is the question of the precise addressees of societal resilience. Before measures can be developed, it must first be determined to whom they are specifically directed.

### **East-West Divide**

Six of the interviewees (N, M, A) emphasized that the threat perception of the Alliance members is one of the most important indicators for the willingness to enhance societal resilience. Thus, respondents see clear differences in the context of the East-West as well as North-South NATO axis in the EuroAtlantic area. While the north-eastern nations, due to their geographical proximity to a potential adversary, demographic and cultural reasons, and current, but also historical experience, are clearly more amenable to societal resilience, the Southern and Western European NATO countries tend to reject these developments.

One N and one M specified in this context that these measures are primarily about involving citizens more in national defence efforts ("hard defence issues"). This is more likely to be undesirable in the Southern and Western European NATO states because countries that traditionally involve their society more in decision-making processes (e.g. Northern European countries) have a lower cultural reluctance towards civil protection structures and a higher responsibility for national security issues. Four persons (N, M, A) stated that the citizens of the Southern and Western

European NATO societies would deal with national security challenges only little or not at all. This is mainly a cultural problem.

However, three interviewees (N, M, A) said that there are common approaches to developing measures to promote societal resilience (“soft defence issues”). All NATO countries agree that their citizens must become more resilient to misinformation and disinformation campaigns. Furthermore, NATO societies should be made more aware of cyber and hybrid threats.

Three participants (N, M, A) went on to say that one of the main challenges was to explain to Alliance citizens that building (societal) resilience and redundancy do not mean militarizing society.

### **COVID-19 Lessons Learned**

Seven respondents (N, M, A) agreed that one of the identified core challenges of the pandemic was dealing with mis- and disinformation campaigns. The destabilising effect (e.g. loss of confidence in the government, etc.) of these campaigns on Alliance societies had been made clear once again.

One N said that a central pillar of NATO’s societal resilience policy is the fight against misinformation and disinformation. This will primarily involve the development of effective measures and capabilities to promote awareness, identification, assessment, and management of negative information activities aimed at exploiting the vulnerabilities of societies in NATO countries.

One person (M) further explained that the pandemic had brought forward new forms of hybrid activities, such as vaccination diplomacy. One scientist also explained that the frequency of cyberattacks had increased significantly during the pandemic. This also increases the risk of critical infrastructure facilities becoming targets of attacks by state or non-state actors.

Four people (N, M, A) explained that the consequences of the pandemic had above all highlighted the sectoral interdependencies between the individual sectors and fields of the Alliance economies. This means, for example, that a disruption in the transport sector can have a massive impact on other critical parts of the economy and society. This also applies across countries and borders.

Four interviewees (N, M, A) also identified the dependence on foreign supply chains as a challenge. Especially at the beginning of the pandemic, it became apparent that most production capacities for medical protective equipment (masks, etc.) were no longer located in Europe and were therefore not immediately available.

One A clarified that our current economic system in terms of the “Just in Time” model is not suitable to deal with strategic shocks and crises of the magnitude of the COVID-19 pandemic. Therefore, moving to a “Just in Case” model would allow quick action in times of crisis through some stockpiling and emergency preparedness. Two other persons (A) concurred with this view in that way that they also considered it necessary for states to increase their reserve capacities in terms of the supply of daily necessities and medical equipment. One M further explained that there must be adjustments in the BLR’s “ability to deal with mass casualties”.

It is not only about failures, but the health system must be looked at holistically. In addition to promoting civilian resilience, NATO must not lose sight of military resilience. One N and one A clarified that it is elementary to involve the population more in civil protection. This could be done, for example, through extended first aid training, so that civilians can be trained to act as first responders. Another low-threshold proposal was to sensitize the population to crisis preparedness with the help of information leaflets and thus make them more resilient, in line with the holistic “whole of society approach”.

Four respondents (N, A) said that the COVID-19 pandemic had highlighted the need to intensify cooperation at both international and national levels. At the international level, exchanges should be intensified, especially between the EU and NATO.

At the national level, interdepartmental planning and communication must be promoted, as well as general coordination between the micro (local level), meso (regional level), and macro (state level) levels of the political systems. In addition, civil-military cooperation needs to be strengthened.

Interpreting the results of the interviews, the following summary can be made.

From the impact of the COVID-19 pandemic, it can be clearly analysed that the Allied countries were hardly able to contain and counter the spread of misinformation and disinformation campaigns. The lack of societal resilience in this area has a negative impact on NATO societies and, in addition to the direct effects of the pandemic, destabilizes them.

Furthermore, the pandemic once again very clearly showed that there are significant economic-sectoral interdependencies. Although this was already known in expert circles during the development of the BLR, COVID-19 clearly demonstrated to the general public the cascading effects that result, for example, from the loss of a large part of the transport sector. It is important to clearly analyse and name the interdependencies and then create redundancies.

The same applies to the dependence on foreign supply chains. It has become clear that the functioning of NATO countries is heavily dependent on the functioning of supply routes. This includes dependence on system rivals such as China, especially in economic terms, or Russia in terms of energy supply. The aim should be to promote the diversification of supply chains. In addition, in particular critical sectors, consideration should be given, jointly within the NATO (and the EU), to repatriating production capacities to Alliance countries. The radical proposal to replace the “Just in Time” model, which is widely practised in the economy but not very resilient, with a “Just in Case” model can also be seen in this context. However, the principle of proportionality or “acting with a sense of proportion” should apply here. It is not desirable and, according to the logic of a democratic market economy, hardly possible to change an entire economic system. However, incentives should be set for key sectors and industries by policy-makers to enable a certain level of stockpiling, in cooperation with government agencies, in order to strengthen the resilience of the state as a whole.

In conclusion, the COVID-19 pandemic showed a clear need for optimisation in the coordination and consultation processes. This applies to both the national and



international levels. At the international level, this applies above all to the intensified cooperation between NATO and the EU. Therefore, the existing discussion and dialogue formats should be further expanded and deepened.

### **6.3 Module 3: Policy**

#### **Concrete Measures and Capabilities**

According to five participants (N, M, A), NATO should motivate its member states to enhance their strategic communication capabilities with their citizens. The population should be more informed, sensitized, and prepared about possible threats and dangers.

Four of the respondents (N, M, A) are in favour of NATO encouraging the nations of the alliance to set up national education programmes aimed at strengthening citizens' media literacy. This would mean teaching citizens what misinformation and disinformation are, how to deal with such news and information, and how to properly identify and analyse sources.

Seven respondents (N, M, A) claimed that the citizens of NATO societies should be more involved in efforts to enhance societal resilience. To this end, NATO should encourage its member states to involve their populations in the planning and decision-making processes for national civil preparedness.

In addition, four people (N, M) suggested that NATO or the CEPC should develop blueprints and recommendations based on the "Total/Comprehensive Defence" model of the Scandinavian countries. This model combines the capacities of the national armed forces and the society of a state in a comprehensive whole of society approach to national security intended to deter an attack by making a target state a very challenging and resilient prospect for an aggressor.<sup>164</sup> These, then generalized but tested concepts and ideas, could be implemented by NATO countries at their own request and thus further increase their societal resilience. In this context, two A pointed out once again that promoting resilience is a mostly civilian task, that NATO and the national armed forces only have a support role, and that the government, universities, and civil society must take the lead.

Four respondents (M, A) consider the implementation of regular cross-stakeholder exercises to train the handling of strategic shocks or crises, identify optimization potentials, and strengthen cooperation as another important aspect that NATO should convey to its member states. One A cited an example from the Czech Republic, where a joint exercise was developed between the armed forces and relevant players in the Czech industry. The aim was to intensify cooperation against hybrid threats and thus strengthen the Czech Republic's resilience. NATO

---

<sup>164</sup> Wither, J.K. 2020, p. 61.

could create a kind of compendium of similar exercises. Allies could access this and transfer the exercises to their national circumstances and adapt them accordingly.

Two interviewees (M, A) said that they thought it would be useful to use the expertise of the NATO accredited Centres of Excellences. This way, they could possibly develop courses and training programmes for member states and support exercises. One A particularly highlighted the new Resilience Centre of Excellence in Romania, which has so far only been operated nationally but is striving for close cooperation with NATO and the EU.

Two N and two M explained the evaluation of the resilience of NATO countries based on the biennial Civil Preparedness Report as part of the NATO Defence Planning Process. In this way, any gaps and needs for optimization could further be identified. One N added in this context that countries should continue to be encouraged to share confidential data from the reports. A peer-to-peer review process could thus incentivize states to address challenges in the relevant areas more quickly and allocate more resources in the course of comparison with partner nations.

In order to effectively promote (societal) resilience, five participants (N, M, A) called for close cooperation between the EU and NATO. In contrast, the EU has the possibility to use legal instruments that are binding in nature, as well as financial resources to promote resilience. One M stated it was important to have only one resilience framework within which the approaches of NATO and the EU were complementary.

In order to deal with the challenges of misinformation and disinformation campaigns in the Alliance, member states sensitized and, above all, informed citizens. Therefore, member states should strengthen their capacities for strategic communication with the population. States must be able to communicate information to citizens quickly, accurately, and comprehensively in order to effectively counter mis- and disinformation. In addition, there is a long-term and far-reaching measure of strengthening media literacy among the population. It is important to teach citizens how they can check sources, what misinformation and disinformation actually are, and how they can deal with them. It is important to reach all social and age groups. Therefore, the members of the Alliance should set up national education programmes that start at school and continue through adult education institutions and other public institutions such as libraries.

Critically, however, it should be noted in this context that the fight against misinformation and disinformation is only one side of the coin. Most of the time, these campaigns are based on the exploitation of fault lines that already exist within society. It is therefore important that countries close these fault lines as best they can, but this is not an issue for NATO.

Furthermore, citizens must be made more aware of national security issues. This can be achieved through increased involvement in political discussion and decision-making processes in this area. Some countries have also called for NATO to develop a generalized concept based on the "Total/Comprehensive Defence" model to increase citizen involvement. This is to be supported, but the implementation of such a model should remain voluntary, as it has been the case so far.

Furthermore, the member states should be encouraged to conduct cross-stakeholder exercises and thus involve socially relevant actors within the framework of a “whole of society” approach. NATO should catalogue these exercises in a generalized form and enable allies to adapt them to national conditions and circumstances.

The last field of action is enhanced cooperation with the EU. It is essential to use the EU’s financial and legal resources in a harmonized way with NATO in the area of resilience. Therefore, existing dialogue and exchange formats should be consistently expanded and deepened in order to ensure a complementary resilience framework.

#### **4th Core Task**

Two of the interviewees (M, A) said that strengthening resilience should be anchored in NATO’s new Strategic Concept as a fourth core task. M pointed out that this would be a good way to give more weight to Article 3 of the NATO Treaty within the Alliance. Furthermore, this would also be in line with policy developments within the EU, which are also about to assign more importance to resilience. One A argued that resilience is the basis for NATO’s other core tasks. However, it is a different dimension of security that needs to be considered separately. Therefore, it needs special attention, which would be given if resilience were to become NATO’s fourth core task.

Four of the respondents (N, M, A) rejected the idea that resilience should be elevated to NATO’s fourth core task. Three interviewees (N, M) saw resilience in differentiated forms and with varying relevance as the basis for fulfilling the other core tasks. Therefore, there would not be a need for a new, separate core task, but resilience implications should be reflected in each of the three core tasks. One N noted that NATO’s core tasks are currently very well balanced and that it would therefore be politically very complex to develop a fourth pillar. Disagreeing with a fourth core task, two other participants (N, A) saw resilience primarily anchored in the first core task: “collective defence”, as resilient state structures form the backbone for a successful defence of the NATO states. In addition, there is the deterrent character that resilient states exude towards potential aggressors.

Neutrally replying four respondents (N, M, A) agreed that NATO needs to do more in the area of resilience and that this should definitely be strongly reflected in the Strategic Concept, but whether this means that resilience should be elevated to the fourth core task is still unclear.

One A expressed concerns that NATO has only limited options in resilience policy and that it would therefore be more important to involve the member states more. National governments, economies, and societies are ultimately responsible for implementing resilience measures.

Interpreting the result, it is clearly more complex whether NATO should include resilience, as part of the revision of the new Strategic Concept, as a fourth core task alongside collective defence, crisis management, and cooperative security. The argument in favour of inclusion is that resilience is a basic condition for fulfilling the other core tasks. The Resilience Commitment 2021 and the ambitions of NATO 2030 consequently see resilience as one of the pillars and an important part of

NATO's response to the changing security landscape in the coming decade. In addition, the political significance as a core task can have a positive impact on the will-building process to promote resilience in the member states. This qualifies resilience as a core task in its own right.

This is contradicted by the fact that resilience is primarily a national matter and the NATO only has a supporting and coordinating role. Classifying it as a core task would not adequately reflect this competence. In addition, there are some voices that see resilience as a basic prerequisite for the other core tasks but do not attach such high importance to it, and therefore there is no justification for a separate core task. Other voices place resilience primarily in the first core task "collective defence" and therefore see no need for action.

This discussion shows that resilience, whether as a core task or not, will be one of the central themes of the concept, which is an explicitly positive development. In the sense of answering the research question, it is to be hoped that resilience will be elevated to the fourth core task; the political effect or the pressure for action that this will trigger cannot be overestimated. Nevertheless, as described in the introduction, the most important thing is that resilience is reflected in the overall concept in accordance with its importance.

## ***6.4 Module 4: Development***

### **Resilient Society from Scratch**

According to seven of the interviewees (N, M, A), a central pillar of a resilient society is an education policy that informs the population about how to deal with classic and modern crises and shocks and also teaches media literacy. This includes, for example, the development of leaflets or physical and online crisis training. In this way, the individual resilience of each citizen can be effectively enhanced. In the area of media literacy, it is important to give children the necessary tools at school to enable them to analyse, question, and assess information, news, and sources. One M explained in this context that it was elementary to reach all parts of society and especially the age groups that are vulnerable on the internet within the framework of an education policy.

Six of the interviewees (N, M, A) pointed out that a resilient society is not possible without empowered citizens participating in political decision-making and planning. Therefore, it is necessary to develop national crisis and emergency plans in cooperation with relevant societal stakeholders.

Two A and one N went on to say that the citizens of NATO countries are a huge untapped resource that countries should use in the context of promoting societal resilience. However, this requires a fundamental paradigm shift: Alliance societies and their citizens should no longer be seen merely as vulnerable individuals who behave in a purely reactive manner and need protection in the event of a crisis but as a potential resource in crisis management. In this context, one M and

one A called for strengthening the individual resilience of each citizen. However, this primarily meant stockpiling emergency supplies. Extensive civil protection and alert systems are part of a resilient society, according to one M. Continuing this comment the ability to recognize threats at an early stage is also part of a resilient society, as one A stated. According to one M, the central principles of crisis management (responsiveness, subsidiarity, cooperation, and similarity) should guide a resilient society in general. In addition, three participants stated that successful and sustainable cooperation between the relevant stakeholders is another basic condition for a resilient society. This includes above all the exchange and coordination between state actors, the private sector, and society at national, regional, and local levels. However, the close socio-economic interdependencies and connections with allied states must also be considered. Therefore, cooperation must also be promoted at the international level.

Three interviewees (A, N) particularly emphasized cooperation with the private sector. As the owner and operator of most critical infrastructures on which the survival of society depends, the private sector must be particularly protected from disruption. Furthermore, the private sector should be encouraged to prepare for possible shocks or crises by creating redundancies in order to minimize the damage to society. The cooperation between all the above-mentioned levels, the implementation of the contingency plans, and the training of the personnel required for this should be trained in regular joint, interdisciplinary exercises.

Eight of the interviewees (N, M, A) considered the democratic system of NATO countries as an elementary prerequisite for a resilient society. Several participants (N, M, A) clarified that democratic mechanisms, principles, norms, and values such as rule of law, openness, transparency, good governance, a sense of community and belonging, unity, respect for and protection of human rights, accountability of the state and clarity about the state's strategic goals and overall interests are very important as basic conditions for a resilient society.

Five interviewees (N, M, A) made it clear that they see a high level of trust of the population in their government and the general government's actions as an existential condition for a resilient society. Thus, citizens would only implement and support government measures if they had a general trust in the government's decisions.

One A stated that, in addition to promoting democratic norms and values, it is important to solve internal societal fault lines and social problem areas through joint dialogue. It happens often enough that misinformation and disinformation campaigns exploit these fault lines to further deepen political polarization and thus the destabilization of society.

## 6.5 *Module 5: Reflection*

### **CIMIC and CMI Contribution**

Seven people (N, M, A) saw CIMIC primarily in a supportive, non-leadership role in promoting societal resilience.

Five of the interviewees (N, M, A) saw the liaison function as the main task of CIMIC. It is important to build up and deepen a civil-military network and to intensify and institutionalize the general dialogue between military and civilian agencies (state authorities, private sector, and civil society). This applies to the strategic as well as the regional and local levels. In this way, information can be exchanged, and challenges and requirements (both from the military and from civilian partners) can be coordinated in times of crisis. In general, it is important in times of crisis to know who is the responsible body or person, how the respective processes work, and how the stakeholders involved interact with each other. Furthermore, three participants (N, M) noted that within the framework of the liaison activities, the opportunity should be used to explain the military activities to the population or the respective counterpart and to promote understanding. This also promotes mutual trust and general transparency. Based on the liaison function, six interviewees (N, M, A) saw the creation of a comprehensive situation picture of the civilian situation on the ground as an important contribution of CIMIC to strengthening societal resilience. This would ensure that both the military command level had the necessary data and information as a basis for decision-making and that this information as a whole could flow into the overall situation picture of all stakeholders.

Based on the results of the study, the role of CIMIC and CMI in promoting societal resilience is mainly supportive. Nevertheless, CIMIC plays an important role in this framework.

The CIMIC core function “Civil-Military Liaison” and the associated development of a civil-military network at all levels should be emphasized. Especially in times of crisis, it is eminently important to know all relevant stakeholders, but above all to know about their understanding of their roles, the processes, needs, and challenges of the respective organisations. CIMIC can promote and moderate this exchange. This promotes joint cooperation, reduces potential obstacles and fear of contact, and increases transparency and understanding of military activities.

Added to this is the ability to develop a comprehensive picture of the civil environment. Based on this, it enables both the military leadership and the other relevant actors to make evidence-based decisions. Therefore, the role of CIMIC tends to be bigger before the deployment as in the actual deployment (in the context of a collective defence scenario), it is about building good relationships and having a large-scale analysis of the host nation’s structures.

## 7 Conclusion and Recommendations

In order to answer this initial question “what can NATO and its entities do to strengthen the Societal Resilience of its member states?”, the term (societal) resilience was first delimited and defined in general and especially in the NATO context. In essence, the meaning of resilience is about resisting or overcoming abrupt crises and shocks in order to maintain essential functions and thus the system as a whole. Furthermore, NATO’s resilience policy was presented from a historical perspective in order to provide the necessary contextualization to answer the research question.

The exploratory part of the research showed that the respondents have a common understanding of what resilience means in the NATO context – even without an official definition. Nevertheless, the results show that a definition would be desirable. This includes the further illustrative use of the “bounce-back” effect to describe a complex process chain. However, it must be clear that this is not a backward-looking, sudden process, but a future-oriented, long-term adaptation process.

In the context of the question of a perfect resilient society, the two most important basic conditions could be identified, which are, however, interdependently linked to each other: a strong democratic basis combined with a high level of trust in the government and, secondly, well-informed and resilient citizens. This includes promoting the strengthening of democratic mechanisms and institutions but also acting based on values and norms. At the same time, this increases trust in government, which is essential for effective governance in times of crisis. Informed and resilient citizens have an adequate level of media literacy and are well prepared for crises of all kinds (both cognitively and practically).

However, NATO also made it clear in this context that strengthening the resilience of member states is first and foremost a national responsibility. This ensures that each state is able to promote its resilience according to its own requirements and resources. Another important aspect in this context is the increased cooperation with relevant partners, such as the EU, in order to generate synergies and harmonization in the field of resilience. NATO should continue to support the member states as best it can with the help of the means at its disposal, as a platform for resources, ideas, coordination, and discussion. In this context, three main challenges could be identified that constrain NATO in the area of enhancing societal resilience. The biggest and most important challenge has already been explained. NATO is not in the leadership role; member states are. Therefore, all progress is dependent on the political will of member states. The research showed that this can vary widely within NATO. The divergent threat perceptions and historical as well as current experiences provide explanations for the fact that the North and Eastern European NATO partners are clearly more positive about initiatives to promote societal resilience than the South and Western European NATO countries. In this context, it is particularly important that the member states and also NATO address the fears of the societies of the latter states and convince them that strengthening

societal resilience is not a militarization of society. Instead, it is a matter of creating redundancies in key capabilities and capacities. Finally, the addressee problem of societal resilience could be identified. This involves defining which parts of society should be involved in the process of demanding societal resilience and how. This is a challenge for both NATO and the member states.

In order to strengthen the societal resilience of NATO countries, a number of concrete proposals were developed. Implications of societal resilience should be incorporated into each of the seven BLRs. Furthermore, consideration should be given to making resilience a core function in NATO's new Strategic Concept. This could further increase the commitment of member states to allocate material and financial resources in this area. In addition, NATO should encourage member states to develop their national capabilities for strategic communication with their citizens. Rapid access to accurate and reliable information is essential to combat misinformation and disinformation. Furthermore, NATO should develop proposals based on the "Total Defence" model to involve citizens more in national security preparedness. In addition, member states should be encouraged to hold cross-stakeholder exercises that explicitly involve actors relevant to society. Finally, increased cooperation with the EU should be mentioned.

The role of CIMIC and CMI in promoting societal resilience is primarily of a supportive nature within NATO. At the same time, the CIMIC core functions must be continuously fulfilled. The development of a civil-military network is eminently important in order to be prepared for a crisis. In addition, the ability to analyse the structures of the host nation is also very important.

Therefore, the data from the interviews reveal the following recommendations with regard to our starting research question ("What can NATO and its entities do to strengthen the societal resilience of its member states?"):

1. Continuation of NATO's support role for member states as a platform for resources, ideas, coordination, and discussion
2. Development of a generalized "Total Defence" concept for the Alliance
3. Support in solving the "addressee problem" of societal resilience
4. Encouraging member states to diversify their relevant economic supply routes
5. Encouraging member states to develop strategic communication capabilities
6. Encouraging member states to develop media literacy and crisis/shock information programmes
7. Encouraging member states to develop resilience training courses
8. Increased cooperation with the EU
9. Introducing resilience as NATO's fourth core task

As the results of this study show, the enhancement of societal resilience will be one of the central tasks of NATO and its member states in this decade. Only countries that are resilient across all stakeholders will be able to cope effectively with future challenges. Therefore NATO and its member states must continue to strengthen resilience as the first line of defence.



# The Psychological Dynamics of Leadership amid a Crisis



Christos Tamouridis, Miguel Moyeno, and William A. Pasmore

## 1 Introduction

Since the dawn of human civilization, humans have faced dilemmas that have required leaders to navigate groups of people amid crises. History tells stories of leaders that led their civilizations through crises such as famine, disease, drought, natural disasters, and war. Similarly, modern leaders have to lead their respective nations through crises such as political division, (cyber) terrorism, genocide, climate change, and global pandemics. Although the scope and complexity of a crisis may vary, the psychological dynamics a leader experiences when a crisis hits remain consistent. Leaders and how they react to crises are as relevant in history as it is today. Perrow [33] studied the dynamics of leaders facing crisis situations and developed what is referred to as “Normal accident theory,” which contends that we should accept that crises of various kinds are to be expected due to the complexity of systems, as is the mishandling of those crises by leaders. While helpful in pointing out the problem, Perrow’s work was less useful in guiding leaders toward actions to prevent or deal with crisis situations.

This article attempts to clearly define and clarify the different psychological dynamics that a leader will experience during a crisis. We begin the article with a modern crisis that paints a clear picture to the reader of what leaders will experience when a crisis hits. Several psychological dynamics will be discussed and are not limited to bias, ambiguity, lack of structure, decreased team performance due to groups staying paralyzed and avoiding making any decisions, dormant and destructive group dynamics such as “power grabs” and “challenges to authority,”

---

C. Tamouridis · M. Moyeno · W. A. Pasmore (✉)  
Teachers College, Columbia University, New York, NY, USA  
e-mail: [cnt2116@tc.columbia.edu](mailto:cnt2116@tc.columbia.edu); [mam2618@tc.columbia.edu](mailto:mam2618@tc.columbia.edu);  
[pasmore@exchange.tc.columbia.edu](mailto:pasmore@exchange.tc.columbia.edu)

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023  
K. P. Balomenos et al. (eds.), *Handbook for Management of Threats*, Springer  
Optimization and Its Applications 205,  
[https://doi.org/10.1007/978-3-031-39542-0\\_24](https://doi.org/10.1007/978-3-031-39542-0_24)

521

the oversaturation of information, and the pressure of the expectation of having to make a quick and yet correct decision.

## 2 Modern Crisis

As the world welcomed the year 2020, an unexpected and unfamiliar disease rapidly spread throughout the world upon its initial case report in Wuhan, China. Within a short time, the infection rate skyrocketed, and “over one-hundred and thirteen million infections were registered globally, with over two million deaths” ([25], p.1). This unknown disease is what we now know as the Novel Coronavirus 2019 (COVID-19), and it was recognized by the World Health Organization (WHO) as the second pandemic of the twenty-first century [25]. As a global community, we are still dealing with the aftermath of the height of this pandemic because it affected every aspect of modern society.

This global health crisis challenged our economies, governments, societies, and our way of life. Leaders were called upon to navigate their systems through a very volatile, uncertain, complex, and ambiguous (VUCA) environment. This pandemic challenged traditional modes of working and heightened anxieties concerning the ability of organizations to continue operating. As leaders began to experiment with hybrid work to compensate for mandated isolation and quarantines, they began to experience unprecedented difficulties, especially with issues regarding their workforce. Teams did not know how to function virtually, decision-making was made difficult by the lack of helpful information regarding the duration of the pandemic, and for a time, some organizations operated less effectively or were forced to shut down operations altogether. The ambiguity and lack of stability cultivated destructive group dynamics, worsened cooperation, and distanced people from each other. As leaders attempted to cope with these perilous group psychological dynamics, teams were expected to make sound and rapid decisions and perform as well as before the COVID-19 pandemic. The stakes were as high as ever in the previous 20 years, demanding world leaders react quickly and effectively to alleviate the crisis and bring back the status quo. In fact, we now know that a return to the status quo is impossible and that the unanticipated effects of the pandemic on supply chains and the future of work are likely to be permanent. Looking back, the question is, “What might leaders have done differently to anticipate and react to the threats posed by the pandemic or other similar crises?”

## 3 Defining Psychological Dynamics, Crisis, and Leadership

Many definitions exist to define psychological dynamics, crisis, and leadership. Psychological dynamics is an “emotional interpretative tendency that affects the internal dialogue related to a meaningful event. It may influence the development

of positive or negative outcomes after stressor events” [29]. One of Merriam-Webster’s definitions of crisis is “an unstable or crucial time or state of affairs in which a decisive change is impending” and “a situation that has reached a critical phase” [30]. Our definition of leadership is based on several influences. Professor of Psychology and Education at Columbia University, Warner Burke, defines leadership as the act of making something happen that would not otherwise occur through a negotiated social relationship between the leader and his or her followers [5]. Thus, leaders, by definition, are responsible for creating the future realities that people in their organizations experience. Leaders who recognize this and are more comfortable shaping the future rather than simply reacting to threats are also more likely to delay closure to understand the issues more fully before acting [41].

Research on leadership has led to the development of five schools of thought. The five are the trait school of leadership, behavioral, situational, transformational, and character theories [32]. Trait or “Great Man” leadership theories explain that charismatic leaders have specific innate characteristics such as intelligence, self-confidence, determination, integrity, and sociability. In essence, this theory contends that great leaders possess traits that distinguish them from their more ordinary counterparts. In a crisis situation, this theory would contend that success is most highly related to having the right person in charge. However, scientific research has not yet found a strong relationship between the traits of leaders and their success in the role [32].

Behavioral theories of leadership suggest that leader behavior is twofold. It is either aimed at meeting the group’s task requirements and prioritizing the task at hand, or it is aimed at meeting the group’s social and emotional needs and prioritizing people’s concerns over goal accomplishment [32]. Behavioral theories argue that the most effective leaders are those who pay attention to both the task and emotional needs of their followers. While useful conceptually, behavioral theories provide little guidance to leaders who must make difficult decisions in the face of a crisis.

Situational leadership theories propose that leadership styles should match the situation at hand. House’s Path-Goal Theory [18] proposes that leaders can choose from four discreet behavioral styles to match the demands of the situation and their followers. These styles are the following: directive, supportive, participative, and achievement-oriented. Participative leader behavior results in follower satisfaction in situations where the task is nonroutine and for self-directed followers who like to take the initiative. Directive leader behavior produces satisfaction and high performance among followers with high needs for clarity and direction. Supportive leader behavior results in follower engagement in situations where the task is highly structured and the follower needs some guidance. Achievement-oriented leader behavior is good for diligent and conscientious followers and improves performance, especially when followers are committed to specific goals [32]. Situational leadership would dictate that during a crisis, where the task is nonroutine and followers lack relevant expertise, leaders should adopt a more directive style. The problem with this, however, is that leaders are no more prepared to deal with

the crisis than their followers and further need the creativity and commitment of their followers to see the crisis through.

The emergence of transformational leadership as a fundamental approach to leadership began with a classic work by political sociologist James MacGregor Burns titled “Leadership” [7]. It is defined as “the process whereby a person engages with others and creates a connection that raises the level of motivation and morality in both the leader and the follower. This type of leader is attentive to the needs and motives of followers and tries to help followers reach their fullest potential” ([32], p. 264). Bass and Riggio [2] enriched Burns’ model proposing that transformational leaders have idealized influence and charisma by being strong role models. They inspire and motivate their people by communicating high expectations. They try to stimulate their followers intellectually by challenging their own beliefs and asking them to remain creative and innovative. Finally, leaders consider each follower separately and adjust their actions to the specific needs of each follower.

In a crisis, transformational leaders would demonstrate confidence in their followers to deal with the situation and be open to suggestions, both of which are helpful behaviors. However, confidence and openness to suggestions can only go so far in resolving the actual crisis or dealing with the anxieties and doubts that followers experience when leaders have no clear answers to guide them.

Character theories of leadership focus on the ethical and characterological dimensions of the leader. They are thoroughly analyzed in Covey’s *Seven Habits for Highly Successful People*, Greenleaf’s *Servant Leadership*, and Goleman’s *Emotional Intelligence*. Covey’s *Seven Habits* are to be proactive, begin with the end in mind, prioritize, think win-win, seek first to understand, and then to be understood, synergize, and sharpen the saw [9]. Greenleaf’s *servant leadership* tenants are listening, empathy, healing, awareness, persuasion, conceptualization, foresight, stewardship, commitment to growing others, and building community [16]. Goleman’s *Emotional Intelligence* attributes are self-awareness, self-regulation, motivation, empathy, and social skills [15]. These dimensions of character, once developed, serve leaders well across situations, including during a crisis. However, their development must precede a crisis to be of utility during the crisis itself, and their application requires reading the situation correctly to decide which aspects of leadership should be brought to the forefront in the moment.

While the study of leadership provides clues, none of the major theories extant provide the guidance that leaders facing an actual crisis need. As noted above, advances in leadership studies have provided more context and research for leaders and how they should act. Interestingly, the abundance of these studies does not address the psychological dynamics at play during a significant threat situation. We argue that understanding these dynamics allows leaders to read the situation more effectively and make better decisions about how to engage their followers in the moment. What distinguishes our approach from other studies is that we suggest that certain variables exist during every crisis, no matter the complexity or the scope. We contend that leaders in a crisis can diagnose the intense psychological dynamics that will manifest themselves, foresee several dysfunctions within their group or

organization, and proactively prepare themselves to react as effectively as possible, considering all the underlying complexity.

## 4 The LEADER Framework

The framework we propose is an action plan for leaders to establish a sound, accurate, and unobstructed picture of the organization and the broader picture that all relevant stakeholder constituencies can easily fathom. This action plan will enable leaders to understand their organization's psychological dynamics at play in order to set the right conditions for effective and efficient crisis management. The LEADER framework is an acronym and stands for: Leveraging the external environment, Examining (and embracing) the group dynamics, Acknowledging culture, Developing the working group into a team, Enhancing psychological safety, and Running Simon's Normative nonrational decision-making model. We postulate that by following this model, leaders and their teams can be in the best possible position to deal with the impending crisis effectively.

### 4.1 *L: Leverage the External Environment*

In 1936, psychologist Kurt Lewin wrote a simple equation that changed our thinking about people and human behavior [23]. In simple terms, he said that behavior is a function of the person in their environment. In order to accurately determine behavior, Lewin's equation holds that one must consider and examine the environment at the exact moment the behavior occurred. Thus, leaders must understand how to influence perceptions of the external environment if they wish to promote specific behaviors from their people.

Organizations operate in an open environment, meaning they constantly need to interact with their environment to survive. Open systems theory proposes that organizations continually interact with the external environment and are thus affected by external forces that will affect their function [31]. External environmental forces include technology, a changing workforce, social and political changes, marketplace/economic changes, and anything else that can affect an organization's status quo.

During a crisis, leaders must pay closer attention to how the external environment is affecting their organization. Then, they must use the knowledge they gain to help followers make sense of what is happening in ways that allow productive adjustments to evolving conditions to occur.

There are several models that offer guidance on how a leader of a large organization can scan the external environment and proceed to educated analyses and decisions. These models include and are not limited to Porter's Five Forces analysis [34], PESTEL (Political, Economic, Social, Technological, Environmental,

and Legal factors) analysis [1], and the scanning of megatrends (artificial intelligence, demographics, drones, big data, renewable power, technology, generations differences) affecting the broader environment.

The goal of studying the external environment is for the leader to prepare as much as possible for likely future scenarios but also to use history to raise questions about the unknown and unexpected. Risk analysis [8] is a discipline that provides methods for leaders first to identify and then prepare responses to threats not previously identified. While even the most disciplined approaches to risk management may not predict the timing or impact of a specific crisis, the practice of conducting risk assessments will prepare leaders to more quickly formulate appropriate responses based on the work they have previously done. The threat of a pandemic was known by many, for example, but few had practiced the discipline of engaging in risk assessment of how this known threat might affect their organizations and what a viable response to such a threat would require.

## ***4.2 E: Examine (and Embrace) the Group Dynamics***

Group dynamics refer to behavioral and psychological processes that occur inside (intragroup dynamics) or within social groups (intergroup dynamics). A group is two or more freely interacting people with shared norms, goals, and a common identity. A group is not synonymous with a team because teams are a small number of people with complementary skills who hold themselves mutually accountable for a common purpose, goal, and approach [21]. Individuals in groups experience hopes and fears manifested in their unconscious and interpersonal dynamics. These dynamics include identity, control, influence, needs and goals, acceptance, and intimacy [37].

According to Wilfred Bion, a significant contributor to the study of group dynamics, a crisis destabilizes groups and surfaces all the dormant group dynamics that might be covert in the status quo [4]. Group members unable to recalibrate immediately after a turbulent event tend to act as if the work at hand is not the primary priority (go off-task). These groups will find it challenging to stay on task because they are in one of the following destructive states: dependency, fight or flight, or pairing. Dependency is when the group acts like the leader is the only one responsible for the group's work and remains stagnant. Fight or flight is when a group's task is to fight or to flee (avoid) rather than do its actual work. Pairing is when a group finds a pair to "pin" the work on for the future. No work happens in the present, and all look to the pair to solve the group's problems in the future. Therefore, the leader should be cognizant of these three group behaviors and prevent them as early as possible.

Another characteristic of group dynamics is what Marshak [26] called "covert processes." These processes are out-of-awareness, hidden, or unconscious factors that impact individuals and organizations and usually remain unseen, unspoken, or unacknowledged. They include hidden agendas, blind spots, organizational

politics, the elephant in the room, secret hopes and wishes, tacit assumptions, and unconscious dynamics. While some of these processes are well hidden, others are often in plain sight.

For leaders in a crisis, understanding group dynamics and surfacing covert processes allows for more effective engagement of their followers. Leaders who are blind to the emotional reactions of their followers presume that their directives are being heard, interpreted, and acted upon appropriately. Not receiving questions or observing dissent, leaders presume agreement from followers when panic, confusion, or disbelief may be predominant emotions. Clearly, the extent to which followers are fully engaged and onboard with the plans for responding to the crisis will influence the effectiveness of the response.

By taking the time to seek and understand information that speaks to the state of group dynamics and covert processes, leaders facing crises are able to “read the room” more effectively and address issues that might otherwise slow or prevent the desired actions to be taken. Leaders who are skilled in these observations will recognize how the lack of psychological safety [12] will hinder the higher-level functioning of individuals as their emotions are turned toward survival needs [27].

While leaders cannot guarantee that the organization will survive the crisis, being transparent about the situation and acknowledging concerns can help redirect energy toward finding solutions. Meeting followers where they are instead of assuming they are in a place that allows them to jump into action allows leaders access to the commitment that is needed to bring the resources followers possess to fight the fire.

Finally, we should address the relationship between power and leadership that will affect leadership during times of crisis. The power of leaders will be challenged during a crisis because such events breed instability and chaos. According to French and Raven [14], leaders derive power over followers from several sources. These include legitimate power or power based on position, expert power or power based on special knowledge and expertise, and referent power or power based on admiration of others. In a crisis, leaders should rely on legitimate power to engage their followers in deciding how best to address the situation if time allows. Rather than claiming expertise that they do not possess, leaders should rely on referent power to influence followers to stay and work through the crisis by being open, humble, and respectful of the feelings that their followers are experiencing. Claiming expertise that they do not have or using their legitimate power to order followers to take actions that followers do not support will undermine the ability of leaders to deal as effectively as possible with the crisis situation.

### ***4.3 A: Acknowledge Culture***

Organizational culture is “the set of shared, taken-for-granted implicit assumptions that a group holds and that determines how it perceives, thinks about, and reacts to its environment” [36]. Another definition, according to Burke and Litwin [6], is “the collection of overt and covert rules, values, and principles that guide organizational

behavior and that have been strongly influenced by history, custom, and practice.” Therefore, culture determines the actual way people will react to an unexpected threat or event.

The function of culture is fourfold: to provide a shared organizational identity, a sense-making device, a means for collective commitment, and, finally, social stability system. Leaders must assess how the crisis will be viewed through the prism of history, values, communication, and socialization and understand that culture is communicated mostly indirectly by stories, rituals, material symbols, and language. The basic underlying assumptions, the taken-for-granted beliefs [36], perceptions, thoughts, and feelings, will be the ultimate source of data for grasping the natural way of dealing with the organization’s problems. A crisis, since it is an abrupt event, will most likely affect the organization’s climate; thus, its cultural way of thinking and acting will remain in place. Leaders must therefore attend to their organization’s culture *before a crisis occurs*. Once a crisis hits, it is unrealistic to expect that a culture of collaboration, self-sacrifice, creative innovation, or openness to change will suddenly emerge, despite the clear need for such things. While followers may agree that these acts are needed, they will have little experience in practicing them, limiting the effectiveness of their attempts to do so.

In contrast to organizational culture, organizational climate is “the collective current impressions, expectations, and feelings of the members of local work units” [6]. A crisis will impact the organization’s climate and will push the organization to react unconsciously through the lens of its engrained organizational culture. Therefore, a leader should know that even if their team climate is good, they should not relax. Instead, they should be open to the previously mentioned indirect manifestations of the organization’s engrained culture.

Values are concepts or beliefs that pertain to desirable end states or behaviors that transcend situations and guide the organization’s selection or evaluation of the behavior of events. A leader armed with this information should leverage espoused and enacted values of the organization to help the organization navigate the current crisis. The leader should play to the organization’s strengths and past accomplishments in order to build confidence on the part of followers regarding their ability to respond to the situation at hand. A leader should tap into the organization’s basic underlying assumptions that lay dormant in the organization’s slogans, goals, acronyms, sayings, stories, legends, and myths to help the organization use these values as the ultimate source of action. Examples of values that a leader should call to action during a crisis include teamwork, participation, commitment, loyalty, and high performance. The ability to tap into the organization’s primordial values will enable it to find strength in an unbroken chain of history that traces its origins to its founding vision, mission, and purpose. During a crisis, a leader must harness the organization’s cultural values; communicate the culture through stories, rituals, material symbols, and language; and channel this collective effort toward the crisis that threatens the organization’s very existence.



#### ***4.4 D: Develop the Working Group into a Team***

Before stepping into how to transform a working group into a team, it is crucial to clarify the two terms since they are not the same. Katzenbach and Smith [21] describe a working group as a collection of people with a strong and focused leader, individual accountability, and individual work products. According to Kinicki [22], “teams are collections of two or more individuals whose tasks and responsibilities depend on the other members, are collectively accountable for the performance and outcomes associated with their work and work together for the time required for tasks completion.” Therefore, the crucial distinction between a working group and a team is that team members are committed to a collective purpose and to one another in serving that purpose [20].

However, analyzing different kinds of crises globally and their respective handling, we observe that the people responsible for dealing with a crisis resemble a working group more often than a team. They seem more interested in delivering individual results without being committed to a greater coping plan. Respectively, we witness people in charge act primarily as managers and less as leaders. They seem more preoccupied with micromanaging the situation than looking at it from a broader lens. Thus, their influence is shallow, and the actions they take do not result in the coming together of individuals who must collaborate in order for the organization to respond effectively to the threat.

The shift from a manager to a leader and from a working group to a team is neither easy nor simple. We are dealing with a profoundly demanding endeavor since the leader will have to face a very complex situation and, at the same time, lead among a group of professionals – decision-makers in their respective fields – and provide guidance and clear direction. Thus, the following described mechanics aspire to enhance the leader’s capabilities of building a nimble and efficient team to ensure the most effective outcomes.

#### **The Core Characteristic of a Team**

As noted above, the core characteristics that define a team are not present in every group or assembly of people. Therefore, whoever aspires to build a strong team should ensure that all of the following characteristics are present in their team. A team is a collection of people that share a social identity as a unit, have common goals, and are interdependent since they are all responsible for the byproducts of their outcomes. They experience constructive or problematic group dynamics and have clear boundaries from the outer environment. Finally, they have distinct and complementary roles in that the sum of all the members’ efforts leads to accomplishing the initially agreed-upon goal [3, 40].

## **The Mechanics of Turning a Working Group into a Team**

Hackman (1989, as cited in Khan, 2008) defines team effectiveness by two criteria: high performance and optimal team processes. Team performance is measured by the products that meet or exceed performance standards and those who receive or evaluate those products. Team processes are defined as interactions among group members that enhance their abilities to work together as a performing unit. Mathieu and Rapp [28] contend that many teams jump directly into performing the alleged goal without taking time to address how they will manage their team processes. Therefore, that results in low team effectiveness in the short term as well as in the long run.

Amid crisis, and for the best possible outcomes, the leader should take advantage of the volatile circumstances and act rapidly. Doing so would be facilitated by having an effective team in place prior to the occurrence of the crisis. To create an effective team that will be better prepared to manage a crisis, the leader should follow the advice of Kahn [20]. Kahn proposes a blueprint of processes to help a group of people evolve into a successful team and achieve their goals. These processes are the following: (a) crafting the mission statement, (b) setting the initial structures right, (c) activating systems of feedback, (d) clarifying how leadership and influence will be exercised, and (e) agreeing to decision-making processes.

### **Crafting the Mission Statement**

What do people expect from the leader? What is (are) the specific goal(s) of the leader that aspires to achieve? How many of them can he or she realistically address, and how can he or she prioritize them?

These are fundamental questions that should be addressed before dealing with actual problems. How the leader will define the team's goals and success is paramount to how he or she will develop the team. According to Locke [24], the more specific or explicit the mission, the higher the performance. Thus, the leader should initially strive to make the team's mission as straightforward as possible to ensure laser-like focus on the required results.

### **Set the Initial Structures Right**

Consequently, the leader should set the proper structure so the team can perform at its best. The BART model, an acronym for boundaries, authority, roles, and tasks, is valuable for setting the right conditions for proper team development [17].

The leader should start by creating clear boundaries between the team and the external environment. The team must remain in control of the unobstructed flow of millions of bits of information, which often proves to be white noise. The boundaries should be permeable enough for the right amount of processed information to be used and analyzed properly and efficiently. Second, he or she must assign distinct

roles to each team member and clarify how the team will be led. Optimally, all team members should agree on how the team will be led and managed. Finally, the leader should determine the task to be done and divide it among the members.

The last part concerns setting the ground rules (a team charter) for how the team communicates and shares information. It is prevalent in the literature that most problems in a team setting come from communication problems (Blake and Mutton (1968, as cited in Burke [5])). People tend to think that what they convey to the other side is clear. However, it is not, creating misunderstandings and misalignments. After everything is discussed and agreed upon, the team has a shared understanding since everyone knows what they want to achieve and how they will solve any potential problem that will arise.

A team charter is an oral document detailing members' mutual expectations about how the team will operate, allocate resources, resolve conflict, and meet its commitments ([22], p.55). A team charter may help teams adapt and be more resilient, enhancing performance in turbulent environments. Research shows that teams that develop team charters are better able to handle disruptive events, increasing their performance [39].

### **Activate Systems of Feedback**

A team to operate efficiently in the long term is not something easy and will not be done without mistakes. Therefore, the team leader should have some systems of feedback that will realign the team to its correct direction and rectify any mistakes made in the meanwhile. These accountability systems can also help the team's cohesion and bonding. When someone knows that others have their back, it is easier for trust and accountability to be cultivated.

### **Leadership and Influence**

If leadership issues are not addressed early, then a covert hierarchy is created to remove the anxiety of not knowing how members should relate to one another. The leader should discuss early on how the team will be led, for instance, through shared team leadership. Shared leadership is a means to create flexible authority structures and space for each member to lead at specific points in the crisis, according to their strengths.

### **Clarify Decision-Making Processes**

Finally, as we will discuss later in the article, the decision-making processes should be determined from the initial phases of team development. Especially during crises when time is absent and abrupt situations come into play, the team should know beforehand how they will make quick decisions or ones with calculated risk.

#### **4.5 E: Enhance Psychological Safety**

When a crisis hits, an organization struggles to maintain control of the situation and is subject to intense external pressure and severe internal tension. Its leader is suddenly, and for a prolonged period, in the public eye and is the object of criticism by the media. The public would like to know who is responsible, why the crisis happened, and how they can protect themselves. While the leader is trying to deal with the whole situation, he or she should also consider that the full scale of the disaster may still be unknown, and the investigation process may take a long time to reach a conclusion.

The above illustration highlights the need for a strong team effort and contribution from all the members of the leader's team. However intelligent and agile, a single mind cannot process all this amount of information, let alone provide quick and to-the-point solutions. However, it is commonly observed that leaders in similar situations, out of fear of delivering bad news and being reprimanded by their stakeholders or the media, tend to become very centralized in their way of leading the team. They do not give autonomy to their people, and they want to be the ones to decide how the problem will be solved. As a result, team members do not express their opinions openly and prefer to stay silent even if they are the most suitable ones to express an educated opinion.

Social neuroscience research highlights that implementing leadership practices that increase autonomy and intrinsic motivation in employees will increase productivity and promote collaboration [35]. Additionally, the organizational psychology literature posits that the above ill-formed situation can be efficiently solved by creating what Edmondson [11] called "team psychological safety," which is the shared belief that the team is safe for interpersonal risk-taking. More specifically, teams with enhanced psychological safety do not fear talking to their leader, and the time is more equally divided between the members. The term is intended to convey confidence that the team would not disgrace, reject, or punish someone for speaking up. In organizational work teams, team psychological safety is positively connected with learning behavior, which is critical during times of crisis when every viewpoint counts [11]. Delizona, in her article [10], diligently describes the following ways to create psychological safety:

##### **Approach Conflict as a Collaborator and Not an Adversary**

Humans are loss averse, which means we hate losing even more than we love winning. A perceived loss triggers attempts to reestablish fairness through competition, criticism, or disengagement, a form of helplessness. When team members deal with a situation with extremely high stakes, conflict is more than a foregone outcome. An educated team member never engages in a conflict and tries to reframe it into a collaboration by asking questions to understand the disputed issue.

## **Speak Human to Human**

Underlying every team's confrontation are universal needs such as respect, competence, social status, and autonomy. Recognizing these deeper needs naturally elicits trust and promotes positive language and behaviors. Leaders should be the first to respect these needs and lead the rest of the team by example.

## **Anticipate Reactions and Plan Countermoves**

Before proposing an idea to the team, it is crucial to consider how the rest members will react to your messaging, like people feeling attacked on their identity or ego. Skillfully confront difficult conversations head-on by preparing for likely reactions.

## **Replace Blame with Curiosity**

You instantly become their adversary when team members detect that you are attempting to blame them for something. According to research at the University of Washington, blame and criticism inside a team intensify defensiveness and disengagement. Instead, embrace a learning mentality, acknowledging that you might not have all the information the other team member has.

Another construct that is a byproduct of a team with psychological safety is voice climate. Voice climate is defined as shared group member perceptions of the extent to which they are encouraged to engage in speaking up. Since doing so challenges the status quo, team members are more likely to assess the risks of engaging in a dialogue with their leader. Further, since aggressive supervisor behavior may cause harm to the employees, the stakes are likely too significant to engage in proactivity, which may enhance exposure to that risk. As group members perceive that they are encouraged to speak up and make suggestions, they are likelier to do so. Voice climate is positively related to group performance, suggesting that higher an enhanced voice climate increases group effectiveness [13].

## **4.6 *R: Run Simon's Normative Nonrational Decision-Making Model***

In times of crisis, we do not have the luxury of using several known decision-making models, such as rational or evidence-based. The main reason is that the leader will have very little time at their disposal, a million bits of information to consider, and much-contradicting information that will hinder their work. Thus, the best solution is the use of a nonrational model. Nonrational models are typically built on the assumptions that decision-making is uncertain, often based on unpredictable

decision-making, decision-makers lack comprehensive knowledge, and managers struggle to make optimum judgments.

Herbert Simon [38] proposed the Normative Model (Satisfactory is Good Enough) to describe managers' decision-making processes. A decision maker's restricted rationality directs this process. According to the concept of bounded rationality, when decision-makers make decisions, they are "bounded" or confined by a range of restrictions [22].

Bounded rationality is caused by any human attributes and internal and external resources that impede rational decision-making and a lack of knowledge. Personal qualities include personality and the human mind's finite capability. Finally, bounded rationality causes managers to collect manageable quantities of information rather than optimal amounts of knowledge. Managers find it harder to uncover all viable alternative options due to this behavior. In the long run, the limits of bounded rationality force decision-makers to satisfy by failing to analyze all feasible options. Satisficing is selecting a solution that fulfills some basic requirements and is "good enough." It addresses issues by generating solutions that are satisfactory rather than optimum.

### **Potential Problems in Team Decision Making**

In this section, the most common problems that hinder effective team decision-making will be analyzed, which are not limited to the domination of a few participants, goal displacement, covert decision-making rules, and groupthink.

*A Few Dominant Participants* The quality of a group's decision can be influenced by a few vocal people who dominate the discussion. This is particularly problematic when the vocal person is perceived as a powerful individual.

*Goal Displacement* When the group is evaluating alternatives, secondary considerations such as winning an argument, getting back at a rival, or trying to impress the boss can override the primary goal of solving a problem. Goal displacement occurs when a secondary goal overrides the primary goal.

*Covert Decision Rules* All decisions are not of the same importance and do not require buy-in from all members. There are situations in which the team should authorize specific experts or subgroups to make decisions. However, each team member should be fully aware of the decision-making structure that is in place. Otherwise, misunderstandings, frustrations, and disagreements are likely to arise. The leader can only achieve clarity on the decision-making processes by openly discussing and agreeing on where authority should be located on each decision.

*Groupthink* Groupthink describes a decision-making process in which group members go along with what seems to be a consensus position, even though that position is not the wisest course. Groupthink causes groups to make irrational decisions that do not fit available data. Members ignore their doubts, conforming to prevailing opinions because they do not wish to derail the decision toward which the group is

heading. According to Janis [19], the three primary causes of groupthink are team cohesion, isolation, and strong leadership.

Operating during a crisis means that leaders will never have the complete information they desire to direct their team and organization to undertake an ideal response. Depending on the time allowed to act, leaders may need to make quick decisions that they know are likely to be imperfect and therefore require redirection in the future. The difficulties posed by the lack of complete information can be further exacerbated by poor team dynamics, resulting in less effective responses that may put the organization's very survival at risk. Therefore, we advise leaders to recognize and shape the dynamics of their teams before crises arise.

## 5 Conclusion

A crisis is a destabilizing event that will unearth covert psychological dynamics and, left unchecked, will erode trust and result in decreased organizational effectiveness. With careful thought, a leader can respond to a crisis in the most effective, agile way possible by utilizing the LEADER framework. Our proposed framework is designed to help leaders focus on the essential psychological dynamics that will play out within their organization. A leader should carefully examine all its proposed tenants and use discretion in applying it to their organization and situation. The fact remains that leading amid a crisis is complex, and how leaders respond to it will be judged based on their decisions and outcomes. Undoubtedly, leaders need to embrace the psychological dynamics that will heighten during such destabilizing events yet find solace that the LEADER framework will provide a practical lens to anticipate and identify these psychological dynamics as expected. A leader cannot anticipate every exigency but can anticipate the baseline psychological dynamics that, when hampered by a crisis, will derail the leader and the organization's ability to respond, adapt, and thrive.

## Bibliography

1. Aguilar, F.J.: *Scanning the Business Environment* (1st THUS). Macmillan (1967)
2. Bass, B.M., Riggio, R.E.: *Transformational Leadership*. Psychology Press (2006)
3. Benishek, L.E., Lazzara, E.H.: Teams in a new era: some considerations and implications. *Front. Psychol.* **10**, 1006 (2019). <https://doi.org/10.3389/fpsyg.2019.01006>
4. Bion, W.R.: Experiences in groups: I. *Hum. Relat.* **1**(3), 314–320 (1948)
5. Burke, W.W.: *Organization Change: Theory and Practice*. SAGE Publications (2017)
6. Burke, W.W., Litwin, G.H.: A causal model of organizational performance and change. *J. Manag.* **18**(3), 523–545 (1992). <https://doi.org/10.1177/014920639201800306>
7. Burns, J.M.: *Leadership*. Harper & Row, New York (1978)
8. Cochrssen, J.J., Covello, V.T.: *Risk Analysis: A Guide to Principles and Methods for Analyzing Health and Environmental Risks*. DIANE Publishing (1999)

9. Covey, S.R., Collins, J., Covey, S.: *The 7 Habits of Highly Effective People: 30th Anniversary Edition (The Covey Habits Series) (Anniversary)*. Simon & Schuster (2020)
10. Delizonna, L.: High-performing teams need psychological safety: here's how to create it. *Harvard Business Review*. (2017), August 24. Retrieved September 12, 2022, from <https://hbr.org/2017/08/high-performing-teams-need-psychological-safety-heres-how-to-create-it>
11. Edmondson, A.: Psychological safety and learning behavior in work teams. *Adm. Sci. Q.* **44**(2), 350–383 (1999). <https://doi.org/10.2307/2666999>
12. Edmondson, A.C.: Teaming across boundaries [E-book]. In: Edmondson, A.C. (ed.) *Teaming: How Organizations Learn, Innovate, and Compete in the Knowledge Economy*, pp. 82–93. John Wiley & Sons (2012)
13. Frazier, M.L., Bowler, W.M.: Voice climate, supervisor undermining, and work outcomes. *J. Manag.* **41**(3), 841–863 (2012). <https://doi.org/10.1177/0149206311434533>
14. French, J., Raven, B.: The bases of social power. In: Cartwright, D. (ed.) *Studies in Social Power*, pp. 259–269. Institute for Social Research, Ann Arbor (1959)
15. Goleman, D.: *Emotional Intelligence: 25th Anniversary Edition*. Bloomsbury Publishing (2020)
16. Greenleaf, R.K., Spears, L.C., Covey, S.R.: *Servant Leadership: A Journey into the Nature of Legitimate Power and Greatness*. Amsterdam University Press (2002)
17. Hirschhorn, L.: Beyond BART (boundaries, authority, role and task): creative work and the developmental project. *Organ. Soc. Dyn.* **18**(1), 41–61 (2018)
18. House, R.J.: A path goal theory of leader effectiveness. *Adm. Sci. Q.* **16**(3), 321–339 (1971)
19. Janis, I.L.: *Victims of Groupthink: A Psychological Study of Foreign-policy Decisions and Fiascoes*. Houghton Mifflin (1972)
20. Kahn, W.A.: *The Student's Guide to Successful Project Teams*, 1st edn. Routledge (2008)
21. Katzenbach, J.R., Smith, D.K.: *The Wisdom of Teams: Creating the High-performance Organization*. Harvard Business School, Boston (1993)
22. Kinicki, A.: *Organizational Behavior: A Practical, Problem-Solving Approach*, 3rd edn. McGraw-Hill Education (2020)
23. Lewin, K.: A dynamic theory of personality: selected papers. *J. Nerv. Ment. Dis.* **84**(5), 612–613 (1936)
24. Locke, E.A.: Motivation through conscious goal setting. *Appl. Prev. Psychol.* **5**(2), 117–124 (1996). [https://doi.org/10.1016/s0962-1849\(96\)80005-9](https://doi.org/10.1016/s0962-1849(96)80005-9)
25. Mallah, S.I., Ghorab, O.K., Al-Salmi, S., Abdellatif, O.S., Tharmaratnam, T., Iskandar, M.A., Sefen, J., Sidhu, P., Atallah, B., El-Lababidi, R., Al-Qahtani, M.: COVID-19: breaking down a global health crisis. *Ann. Clin. Microbiol. Antimicrob.* **20**(1), 35 (2021). <https://doi.org/10.1186/s12941-021-00438-7>
26. Marshak, R.J.: A model for understanding covert processes. In: *Covert Processes at Work: Managing the Five Hidden Dimensions of Organizational Change (Annotated ed.)*, pp. 19–34. Berrett-Koehler Publishers (2006)
27. Maslow, A.H.: A theory of human motivation. *Psychol. Rev.* **50**:370–396 (1943). <https://doi.org/https://doi.org/10.1037/h0054346>
28. Mathieu, J.E., Rapp, T.L.: Laying the foundation for successful team performance trajectories: the roles of team charters and performance strategies. *J. Appl. Psychol.* **94**(1), 90–103 (2009). <https://doi.org/10.1037/a0013257>
29. Mercante, J., Nasello, A.G.: Psychological dynamics affecting traumatic memories: implications in psychotherapy. *Psychol. Psychother. Theory Res. Pract.* **78**(4), 431–447 (2005, December). <https://doi.org/10.1348/147608305x26693>
30. Merriam-Webster. (2022). *Crisis*. <https://www.merriam-webster.com/dictionary/crisis>
31. Morgan: *Images of Organization (Updated edition)*. Sage Publications (2006)
32. Northouse, P.G.: *Leadership: Theory and Practice*, 8th edn. SAGE Publications, Inc (2018)
33. Perrow, C.: *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press (1984)
34. Porter, M.E.: The five competitive forces that shape strategy. *Harv. Bus. Rev.* **86**(1), 25–40 (2008)



35. Rock, D., Cox, C.L.: SCARF<sup>®</sup> in 2012: Updating the Social Neuroscience of Collaborating with Others (2012)
36. Schein, E.H.: Culture: The Missing Concept in Organization Studies. *Administrative Science Quarterly*. **41**(2), 229 (1996). <https://doi.org/10.2307/2393715>
37. Schein, E.H.: *Organizational Culture and Leadership*. Wiley (2016)
38. Simon, H.A.: *Models of Bounded Rationality: Empirically Grounded Economic Reason* (Vol. 3). MIT Press (1997)
39. Sverdrup, T.E., Schei, V., Tjølsen, Y.A.: Expecting the unexpected: using team charters to handle disruptions and facilitate team performance. *Group Dyn. Theory Res. Pract.* **21**(1), 53–59 (2017). <https://doi.org/10.1037/gdn0000059>
40. Velsor, V.E., McCauley, C.D., Ruderman, M.N.: *The Center for Creative Leadership Handbook of Leadership Development, Third Edition, 3rd edn.* Jossey-Bass (2010)
41. Zaleznik, A.: Managers and leaders: Are they different? *Harv. Bus. Rev.* **55**(5), 67–78 (1977)