SPRINGER REFERENCE

Elias G. Carayannis
David F. J. Campbell
Marios Panagiotis Efthymiopoulos
Editors

Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense

Springer

Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense

Elias G. Carayannis • David F. J. Campbell
Marios Panagiotis Efthymiopoulos
Editors

Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense

With 132 Figures and 31 Tables

Springer

Editors
Elias G. Carayannis
Department of Information Systems and Technology Management
School of Business
The George Washington University
Washington, DC, USA

Marios Panagiotis Efthymiopoulos
School of Law
University of Central Lancashire (UCLan Cyprus)
Larnaka, Cyprus

Strategy International
Larnaka, Cyprus

Strategy International
Thessaloniki, Greece

David F. J. Campbell
Department for Continuing Education Research and Educational Management
Centre for Educational Management and Higher Education Development
Danube University Krems
Krems, Austria

University of Applied Arts Vienna
Unit for Quality Enhancement (UQE)
Vienna, Austria

Faculty for Interdisciplinary Studies (iff)
Institute of Science Communication and Higher Education Research (WIHO)
Alpen-Adria-University Klagenfurt
Vienna, Austria

Department of Political Science
University of Vienna
Vienna, Austria

ISBN 978-3-319-09068-9 ISBN 978-3-319-09069-6 (eBook)
ISBN 978-3-319-09070-2 (print and electronic bundle)
https://doi.org/10.1007/978-3-319-09069-6

Library of Congress Control Number: 2018948193

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

Preface

This publication focuses on a new approach reflective in both *interdisciplinary, cross disciplinary, and trans-disciplinary research*. ***Cyber-Development, Cyber-Democracy, and Cyber-Defense (Cyber D3)*** is placed within a comparative framework of examination, analysis, and lessons learned, which acquires further understanding of current and future challenges and threats, considering, at the same time, opportunities, implications, and applications; involving theory and conceptual evolution, to policy orientation and creation, practice, learning, and adaptability.

The unfolding dynamics, among others, of the revolution of knowledge production, innovation application, and informatics and technology poses swift and robust changes reflective through development, democracy, and defense. The Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense reflects as a term and concept this current and future transformation and evolution. The joint phrase of **"Cyber" (D3)** expresses and emphasizes the processes that drive development, democracy, and defense; Cyber D3 subjects are in fact interrelated, cross-linked, overlap with each other, and network with each other. *As such the new complexity on Cyber terminologies and in Cyber policies emerges. It pushes out to new boundaries and borders; pushes our thinking and our practice to a new Cyber-Horizon beyond established structures; and encourages a "thinking beyond the box".*

Washington, D.C., United States — Elias G. Carayannis
Athens, Greece — David F. J. Campbell
Vienna, Austria — Marios Panagiotis Efthymiopoulos
Larnaka, Cyprus
August, 2018

Acknowledgment

Our sincere thanks and our acknowledgment goes to all contributors and authors for their efforts, for their engagement and their contributions. We, together, have created this innovative intellectual work, which is expected to be analyzed, evaluated, discussed, and to be reflected further through academic and professional discourses, dialogues, and fora, academic as well as professional.

As editors, we would also like to thank Springer Publications; the team that worked for the project to be well completed.

The *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense* (Cyber D3) is a most important contribution. It refers to and addresses, among others, the success of a first book on the very same topics that has circulated globally.[1] It now enlarges and complements efforts with new and most important contributions that will certainly be examined and discussed, however, this time on a Handbook. The Handbook reflects the team effort to comprehend and to discuss a diversity of issues in the Cyber-World, subjects that are of significant importance and impact, academic and professional.

Elias G. Carayannis
David F. J. Campbell
Marios Panagiotis Efthymiopoulos

[1]Carayannis, E. G., Campbell, D. F. J., & Efthymiopoulos, M. P. (Eds.). (2014). *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice*. New York: Springer. http://www.springer.com/social+sciences/political+science/book/978-1-4939-1027-4

Contents

About the Editors

Dr. Elias G. Carayannis is Full Professor of science, technology, innovation, and entrepreneurship, as well as Co-founder and Co-director of the Global and Entrepreneurial Finance Research Institute (GEFRI) and Director of research on science, technology, innovation and entrepreneurship, European Union Research Center (EURC), at the School of Business of the George Washington University in Washington, D.C. Carayannis' teaching and research activities focus on the areas of strategic government-university-industry R&D partnerships, technology road-mapping, technology transfer and commercialization, international science and technology policy, technological entrepreneurship, and regional economic development.

Dr. Carayannis has several publications in both academic and practitioner journals, including *Journal of Organizational Behavior*, *Journal of Operational Research*, *Expert Systems with Applications*, *IEEE Transactions in Engineering Management*, *Research Policy*, *Journal of R&D Management*, *Journal of Engineering and Technology Management*, *International Journal of Technology Management*, *Technovation*, *Journal of Technology Transfer*, *Engineering Management Journal*, *Journal of Growth and Change*, *Review of Regional Studies*, *International Journal of Global Energy Issues*, *International Journal of Environment and Pollution*, *Le Progres Technique*, and *Focus on Change Management*. He has also published more than 40 books to date on science, technology, innovation, and entrepreneurship with Springer, CRC Press, Praeger/Greenwood, Palgrave/

MacMillan, and Edward Elgar and has several more projects under contract.

Dr. David F. J. Campbell is a Research Fellow (Senior Scientist) at the Institute of Science Communication and Higher Education Research (WIHO), Faculty for Interdisciplinary Studies (iff), Alpen-Adria-University of Klagenfurt (http://www.uni-klu.ac.at/wiho/inhalt/445.htm); Lecturer and "Privat-Dozent" in Political Science at the University of Vienna (https://politikwissenschaft.univie.ac.at/en/about-us/staff/associate-professors/campbell/); a Quality Enhancement Expert and Quality Researcher at the University of Applied Arts in Vienna (http://www.dieangewandte.at/jart/prj3/angewandte_aris/ main.jart?j-j-url=/_1 and http://www.dieangewandte.at/uqe); and a Project Manager and Researcher at the Center for Educational Management and Higher Education Development, Department for Continuing Education Research and Educational Management, at Danube University Krems (https://www.donau-uni.ac.at/en/universitaet/whois/25849/index.php). He studied political science at the University of Vienna, completing his studies with a doctoral degree in 1996. In 2014, Dr. Campbell received a "Habilitation" (Doctor Habilitatus) from the University of Vienna with a Venia Docendi for Comparative Political Science.

Dr. Campbell lead-authored *The Quality of Democracy* (Palgrave Macmillan, 2018, forthcoming), *Democracy Ranking (Edition 2014): The Quality of Democracy in the World* (Books on Demand, 2015), *Epistemic Governance in Higher Education: Quality Enhancement of Universities for Development* (Springer, 2013), and *Democracy Ranking (Edition 2012): The Quality of Democracy in the World* (Books on Demand, 2012); co-authored *Mode 3 Knowledge Production in Quadruple Helix Innovation Systems: 21st-Century Democracy, Innovation, and Entrepreneurship for Development* (Springer, 2012); co-edited *Arts, Research, Innovation and Society* (Springer 2015), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges,*

Opportunities and Implications for Theory, Policy and Practice (Springer, 2014), *Encyclopedia of Creativity, Invention, Innovation and Entrepreneurship* (Springer, 2013), *Knowledge Creation, Diffusion, and Use in Innovation Networks and Knowledge Clusters* (Praeger, 2006), and *Demokratiequalität in Österreich: Zustand und Entwicklungsperspektiven* (Leske + Budrich, 2002) ("Democracy Quality in Austria"). His articles on knowledge, innovation, knowledge economy, and democracy (knowledge democracy and quality of democracy) have been published in several international journals (citations of his academic work can be followed at Google Scholar: http://scholar.google.at/citations?user=GSNvicMAAAAJ&hl=en&oi=ao). Dr. Campbell teaches (taught) at the University of Klagenfurt, University of Vienna, University of Applied Arts Vienna, and George Washington University in Washington D.C. (Elliott School of International Affairs).

David Campbell is Academic Director of the global **Democracy Ranking** of the *quality of democracy* (http://democracyranking.org/) and Senior Associate Editor (Chief Associate Editor, Associate Editor, Managing Editor) to the following journals and the following book series:

Journal of the Knowledge Economy (JKEC) (Springer), http://www.springer.com/economics/policy/journal/13132

Journal of Innovation and Entrepreneurship (JIE) (Springer Open Source), http://www.springer.com/business+%26+management/entrepreneurship/journal/13731

Journal of Knowledge Management (JKM) (Emerald Publishing), http://emeraldgrouppublishing.com/products/journals/editorial_team.htm?id=jkm

International Journal of Social Ecology and Sustainable Development (IJSESD) (IGI Global), http://www.igi-global.com/journal/international-journal-social-ecology-sustainable/1174

Arts, Research, Innovation, and Society (ARIS) (Springer), http://www.springer.com/series/11902

Professor Dr. Marios Panagiotis Efthymiopoulos is an Associate Professor of International Security and Strategy. He is an internationally distinguished scholar and an expert in diverse fields ranging from traditional affairs of national and international security and strategy to cyber-security and cyber-defense, strategic resilience, information analysis, intelligence, smart cities and national infrastructure, future affairs, and decision–making, among others. His professional expertise includes advising and operational positions, from advising the President of Cyprus through the Geostrategic Council to consulting for international consultancy companies He also works for international organizations such as NATO, and is CEO of Strategy International Think Tank Consulting firm since 2008. His current and past academic positions include senior research fellow at the School of Law, University of Central Lancashire (UCLan) Cyprus, Dean of academic Affairs at Jumeira University, Dubai, UAE; founding Dean of the College of Security and Global Studies, American University in the Emirates, Dubai, UAE; Columbia University's Harriman Institute, New York USA; The Center for Transatlantic Relations, Johns Hopkins University, Washington DC. USA; George Washington University, School of Business and the European Center of Excellence; Washington DC, USA; the Woodrow Wilson Center for International Scholars Washington DC, USA; visiting research fellow at the University of South Florida and visiting lecturer at the University of Cyprus' Department of Social and Political Sciences. Professor Dr. Efthymiopoulos has authored numerous books, articles, and working papers and is a peer review editor/evaluator. He regularly writes for newspapers and comments on national and international TV news groups. He holds a Ph.D. in the Specialization of International Security and Strategy from the University of Crete, Greece. He holds a Diploma from the NATO Defense College (Senior Course 105) in Security and Strategic Affairs, including the Integrated PfP/OSCE Course 04/02, Rome Italy; an M.A. in Advanced International Studies from the Diplomatic Academy of Vienna, Austria; a B.A. (Hons) in International Relations and Politics from the University of Lincolnshire

and Humberside (now University of Lincoln), from Lincoln, UK. His Upcoming research book is titled *Falkon's Maze on Cyber-Security: The Case of the United Arab Emirates (UAE)*, to be published by Springer in the first quarter of 2021.

Contributors

Jawad Hussain Awan Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan

Daniel F. Baltrusaits National Defense College of the United Arab Emirates, Abu Dhabi, United Arab Emirates

Near East South Asia Center for Strategic Studies, National Defense University, Washington, DC, USA

Thorsten D. Barth Political Scientist and Academic Entrepreneur, Vienna Democracy Ranking Organization – Academic Ranking Team, Vienna, Austria

Florian Alexander Boesenkopf influence.vision, iwondo and NoviSmart, Technology Scout for Bosch in Palo Alto, Vienna, Austria

Juergen Braunstein London School of Economics and Political Science, London, UK

Pavol Cabada Political Science, CEIT Internship, Vienna University, CEIT Technical Innovation, Vienna, Austria

David F. J. Campbell Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria

Elias G. Carayannis Department of Information Systems and Technology Management, School of Business, The George Washington University, Washington, DC, USA

Danilo Cupic Ministry of Internal Affairs, Podgorica, Montenegro

José María Díaz-Nafría Faculty of Systems and Telecommunications, Universidad Estatal Península de Santa Elena / SENESCYT - Prometeo, La Libertad, Provincia de Santa Elena, Ecuador

Faculty of Education, Universidad de León, Leon, Spain

Department of General and Interdisciplinary Studies, Munich University of Applied Sciences, Munich, Germany

Marios Panagiotis Efthymiopoulos School of Law, University of Central Lancashire (UCLan Cyprus), Larnaka, Cyprus

Strategy International, Larnaka, Cyprus

Strategy International, Thessaloniki, Greece

Birgit Eigelsreiter Ministry of Health and Women's Affairs, Vienna, Austria

Hamid R. Ekbia School of Informatics and Computing, School of Global and International Studies, Indiana University, Bloomington, Bloomington, IN, USA

Birte Fähnrich Zeppelin University, Friedrichshafen, Germany

Peter Filzmaier Platform Political Communication, Danube University Krems, Krems, Austria

Thomas A. E. Fuchs Political Science (Research Focus: European Union, European Integration), University of Vienna, Vienna, Austria

Matthias Galan Amsterdam, Netherlands

Vienna, Austria

Johannes Göllner Institute of Strategy, Foresight, Risk and Innovation Management, MASARYK University, Socio-Economic Faculty, Brno, Czech Republic

Center for Risk and Crisis Management, University of Natural Resources and Life Sciences, Vienna, Austria

Georg Hanschitz Institute of Education and Innovation, Vienna, Austria

Maria E. Haupt polis – The Austrian Centre for Citizenship Education in Schools, Ludwig Boltzmann Institute of Human Rights, Vienna, Austria

Vahid Heydari Department of Computer Science, Rowan University, Glassboro, NJ, USA

Nathalie Hoffmeister Department of Political Science, University of Vienna, Vienna, Austria

Stefan Hügel Forum Computer Professionals for Peace and Social Responsibility (FIfF), Bremen, Germany

John S. Hurley College of Information and Cyberspace, National Defense University, Washington, DC, USA

Anthony Chukwuemeka Ijeh College of Computer Information Technology, American University in the Emirates, Dubai, UAE

Jonas Kaiser Department for Political and Social Sciences, Zeppelin University, Friedrichshafen, Germany

Berkman Klein Center for Internet and Society, Harvard University, Cambridge, MA, USA

Joachim Klerx Foresight, Research, Technology and Innovation Policy, Austrian Institute of Technology, Vienna, Austria

Hana Korac Ministry of Internal Affairs, Sarajevo, Bosnia and Herzegovina

Hans-Jörg Kreowski Computer Science Department, University of Bremen, Bremen, Germany

Stefan Kuhlmann Science, Technology and Policy Studies Department, Faculty of Behavioural, Management and Social Sciences, University of Twente, Enschede, The Netherlands

Klaus Mak National Defence Academy, Ministry of Defence and Sports, Republic of Austria, Vienna, Austria

Boris S. Manov Political Science, Researcher at University of Vienna, Vienna, Austria

Sofia, Bulgaria

Shahzad Memon University of Sindh, Allama I.I.Kazi Campus, Jamshoro, Sindh, Pakistan

Christian Meurers National Defence Academy, Ministry of Defence and Sports, Republic of Austria, Vienna, Austria

Dietrich Meyer-Ebrecht RWTH Aachen, Institute of Imaging and Computer Vision, Aachen, Germany

Karl H. Müller Steinbeis Transfer Center New Cybernetics, Vienna, Austria

Emanuele Musa Babele, Roumania, Italy

Tuğba Özcan Master of Arts in Political Science, University of Vienna, Vienna, Austria

Spyridon Papastergiou UNIPI Security Lab, Department of Informatics, University of Piraeus, UNIPI, Pireaus, Greece

Andreas Peer Center for Risk and Crisis Management, Vienna, Austria

M2D MasterMind Development GmbH, Vienna, Austria

Annalisa Pelizza Science, Technology and Policy Studies Department, Faculty of Behavioural, Management and Social Sciences, University of Twente, Enschede, The Netherlands

Pythagoras Petratos Said Business School, Oxford University, Oxford, UK

Nineta Polemi UNIPI Security Lab, Department of Informatics, University of Piraeus, UNIPI, Pireaus, Greece

Peter Prah National Defence Academy, Ministry of Defence and Sports, Republic of Austria, Vienna, Austria

Gerald Quirchmayr Faculty of Computer Science, Research Group Multimedia Information Systems, University of Vienna, Vienna, Austria

Stefan Rass System Security Research Group, Institute of Applied Informatics, Universität Klagenfurt, Klagenfurt, Austria

Markus Rhomberg Department for Political and Social Sciences, Zeppelin University, Friedrichshafen, Germany

Alexander Ruser Zeppelin University, Friedrichshafen, Germany

Eldar Saljic American University in the Emirates, Dubai, UAE

Anders Sandberg Oxford Martin Programme on the Impacts of Future Technology, Oxford University, Oxford, UK

Future of Humanity Institute, Oxford University, Oxford, UK

Willi Schlegelmilch Accounting System Standardisation, Schönaich, Germany

Wieland Schneider Die Presse, Vienna, Austria

Tomáš Sigmund Department of System Analysis, University of Economics, Prague, Czech Republic

Nico Stehr Karl Mannheim Chair of Cultural Studies, Zeppelin University, Friedrichshafen, Lake Constance, Germany

Kajetan Stransky-Can Bundesministerium für Wissenschaft, Forschung und Wirtschaft, Vienna, Austria

Dusko Tomic American University in the Emirates, Dubai, UAE

Doris Wilhelmer Center for Innovation Systems and Policy, AIT Austrian Institute of Technology GmbH, Vienna, Austria

Robert F. Xavier Middle East Analyst, ThePoliticalMinds.com, Laguna Hills, CA, USA

Viliam Zathurecky Institute of Strategy, Foresight, Risk and Innovation Management, MASARYK University, Socio-Economic Faculty, Brno, Czech Republic

Feng Zhou Future of Humanity Institute, Oxford University, Oxford, UK

Part I

Cyber-Development

Overview of Cyber-Development

1

Elias G. Carayannis and David F. J. Campbell

Developed and developing economies alike face increased resource scarcity and competitive rivalry. Science and technology increasingly appear as a main source of competitive and sustainable advantage for nations and regions alike. However, the key determinant of their efficacy is the quality and quantity of entrepreneurship-enabled and ICT-driven innovation that unlocks and captures the pecuniary benefits of the science enterprise in the form of private, public, or hybrid goods. In this context, there is ample and growing evidence that intangible resources such as knowledge, know-how, and social capital will prove to be the coal, oil, and diamonds of the twenty-first century for developed, developing, and emerging economies alike (The Global Competitiveness Report 2001–2002, WEF & Harvard CID, NY/Oxford, OUP, 2002.). Moreover, there are strong indications and emerging trends that there are qualitative and quantitative differences between the twentieth- and twenty-first-century drivers of economic growth

E. G. Carayannis (✉)
Department of Information Systems and Technology Management, School of Business, The George Washington University, Washington, DC, USA
e-mail: caraye@gwu.edu

D. F. J. Campbell
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@donau-uni.ac.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_71

(Toward e-Development in Asia and the Pacific: A Strategic Approach for Information and Communication Technology, ADB, June 2001):

> The world economy is in the midst of a profound transformation, spurred by globalization and supported by the rapid development of ICT [Information and Communication Technologies] that accelerates the transmission and use of information and knowledge. This powerful combination of forces is changing the way we live, and redefining the way companies do business in every economic sector. (Carayannis and Sipp 2006, p. 2)

We are currently going through a dynamic era for the economies of the world where a country can transition fast both upward or downward, and this trend has become increasingly more pronounced and in an accelerating fashion during the last decade. This new era is punctuated by (China and the Knowledge Economy: Seizing the twenty-first century, Carl Dahlman & Jean Eric Aubert, WBI, October 2001):

- Development of a service-based economy, with activities demanding intellectual content becoming more pervasive and decisive
- Increased emphasis on higher education and life-long learning to make effective use of the rapidly expanding knowledge base
- Massive investments in research and development, training, education, software, branding, marketing, logistics, and similar services
- Intensification of competition between enterprises and nations based on new product design, marketing methods, and organizational forms
- Continual restructuring of economies to cope with constant change

Specifically, technology and knowledge have become the key factors of production; knowledge is now the basic form of capital. Economic growth is driven by the accumulation of knowledge, and new technological developments create technical platforms for further innovations. These technical platforms are, in turn, drivers of economic growth. Technology raises the return on investment. Information and communications technologies (ICTs) facilitate human exchange, particularly commercial and political transactions, which in turn, develop the base of knowledge capital, and raise the stakes for attaining and sustaining competitiveness in global markets.

Our working definition for the knowledge economy (KE) is as follows:

> The Knowledge Economy is a state of economic being and a process of economic becoming that leverages intensively and extensively knowledge assets and competences as well as economic learning to catalyze and accelerate sustainable and robust economic growth. (Carayannis and Sipp 2006, p. 12)

Our working definition of cyber-development (an alternate, earlier term being e-development) is as follows:

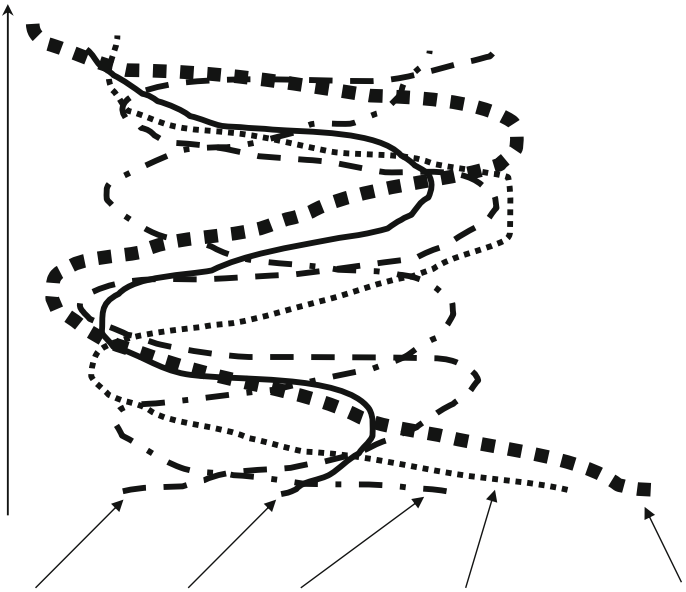
> Cyber-Development is a set of tools, methodologies, and practices that leverage ICT to catalyze and accelerate social, political and economic development or in other words, Cyber-Development is Information-and-Communication Technology-(ICT)-enabled and Knowledge-Economy-(KE)-inspired development that may enable the economies of developing and especially transitioning countries to become Knowledge Economies. This also applies to the advanced economies. (Carayannis and Sipp 2006, p. 12)

Adam Smith defined *land, labor, and capital* as the key input factors of the economy in the eighteenth century. Joseph Schumpeter added *technology and entrepreneurship* as two more key input factors in the early twentieth century. He thus recognized the role and dynamic nature of technological change and innovation as well as path dependencies in shaping the health and future of the economy and moving away from the static approach of neoclassical economics.

Technology brings unprecedented potential to make interactions between the public and the private sector easier, more efficient, and more transparent. The ability of technology to dramatically reduce transaction costs has stimulated the adoption of ICT in many developmental interventions.

The advancement of science and technology (S&T) requires improvements in policy and regulatory environment for the application of S&T to economic development and the identification of potential risks and benefits of new and emerging technologies. Long-term growth depends on creating loci of innovation activities. Weaknesses in national, sectoral, and regional determinants make weaknesses at the level of the enterprise. To globally sustain the knowledge economy will require strengthening in the area of basic and applied research in developing countries and international scientific networking, technology support institutions and science advisory mechanisms, and building human capacity worldwide. *Humanity cannot rely on natural resources or manufacturing for sustainability*. Future viability demands identifying new technologies and applications and encouraging international collaboration to support research in neglected fields.

The theory, concept and model of the "quadruple and quintuple helix innovation systems" (Carayannis and Campbell 2009, 2010, 2014; Carayannis et al. 2012) describes and explains how knowledge production (research) and knowledge application (innovation) are functioning and can be enhanced in advanced economies, but also in the emerging and developing economies. The quadruple helix emphasizes civil society and democracy, and the quintuple helix addresses the environment and ecology (see Figs. 1 and 2). The quadruple and quintuple helix innovation systems also offer references for policy, strategy, practice, and learning, how reform and policy and policy innovation are possible for a betterment and progress of cyber-development in sustainable development, and how the transformation and evolution of economy, society, and democracy into knowledge economy, knowledge society, and knowledge democracy can be approached and processed.



First Helix: Academia / universtities	Second Helix: Industry / business	Third Helix: State / government	Fourth Helix: Media-based and culture-based public; civil society; arts, artistic reseach and arts-based innovation /	Fifth Helix: Natural environment, natural environments of society and economy /
Universities (higher education institutions) of the sciences and of the arts.	Also: creativity economy and creative industries.		culture and innovation culture, knowledge of culture and culture of knowledge, values and life styles, multi-culturalism and creativity, media, arts and arts universities, multi-level innovation systems with universities of the sciences and arts.	social ecology, society-nature interactions, socio-ecological transition.

Triple Helix:	**University-industry-government relations (helices).**
Quadruple Helix, Fourth Helix:	**"Media-based and culture-based public", "civil society" and "arts, artistic research and arts-based innovation" (helix).**
Quintuple Helix, Fifth Helix:	**Natural envrionment, natural environments of society and economy (helix).**

Fig. 1 The quadruple and quintuple helix innovation systems. (Source: Carayannis and Campbell (2014, p. 15), adapted from Carayannis and Campbell (2009, p. 207))

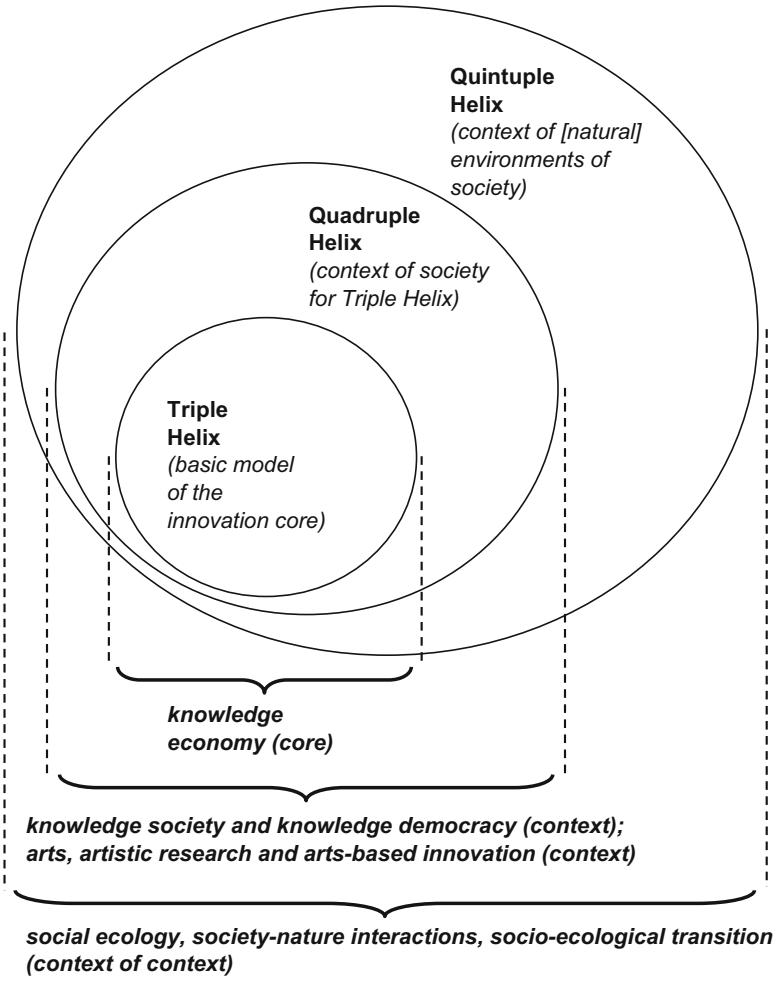


Fig. 2 The quadruple and quintuple helix innovation systems in relation to society, economy, democracy, and social ecology. (Source: Carayannis and Campbell (2014, p. 6), adapted from Carayannis et al. (2012, p. 4))

References

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "Quadruple helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46* (3/4), 201–234. http://www.inderscience.com/browse/index.php?journalID=27&year=2009&vol=46&issue=3/4 and http://www.inderscience.com/search/index.php?action=record&rec_id=23374&prevQuery=&ps=10&m=or.

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed

framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69. http://www.igi-global.com/bookstore/article.aspx?titleid=41959.

Carayannis, E. G., & Campbell, D. F. J. (2014). Developed democracies versus emerging autocracies: Arts, democracy, and innovation in quadruple helix innovation systems. *Journal of Innovation and Entrepreneurship, 3*, 12. http://www.innovation-entrepreneurship.com/content/pdf/s13731-014-0012-2.pdf and http://www.innovation-entrepreneurship.com/content/3/1/12.

Carayannis, E. G., & Sipp, C. M. (2006). *e-Development toward the knowledge economy. Leveraging technology, innovation and entrepreneurship for "Smart" development*. Houndmills: Palgrave Macmillan.

Carayannis, E. G., Barth, T. D., & Campbell, D. F. J. (2012). The quintuple helix innovation model: Global warming as a challenge and driver for innovation. *Journal of Innovation and Entrepreneurship, 1*(1), 1–12. http://www.innovation-entrepreneurship.com/content/pdf/2192-5372-1-2.pdf.

Quadruple and Quintuple Helix Innovation Systems and Mode 3 Knowledge Production

2

Elias G. Carayannis and David F. J. Campbell

Contents

E. G. Carayannis (✉)
Department of Information Systems and Technology Management, School of Business, The George Washington University, Washington, D.C, USA
e-mail: caraye@gwu.edu

D. F. J. Campbell
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@uni-ak.ac.at; david.campbell@aau.at; david.campbell@univie.ac.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_56

Abstract

While for the Triple Helix model the existence of a democracy is not necessary for knowledge production and innovation, the Quadruple Helix is here more explicit. The way, how the Quadruple Helix is being engineered, designed, and "architected," from that it is clear that there cannot be a Quadruple Helix innovation system without democracy or a democratic context. The following attributes and components define the fourth helix in the Quadruple Helix: "media-based and culture-based public," "civil society," and "arts, artistic research and arts-based innovation." By this the fourth helix in the Quadruple Helix represents the perspective of the "dimension of democracy" or the "context of democracy" for knowledge, knowledge production, and innovation. This is particularly true when democracy is to be understood to transcend the narrow understanding of being primarily based on or being primarily rooted in government institutions (within Triple Helix). Civil society, culture-based public, quality of democracy, and sustainable development convincingly demonstrate what the rationales and requirements are for conceptualizing democracy broader. Political pluralism in a democracy coevolves with the pluralism, diversity, and heterogeneity of knowledge, knowledge production, and innovation ("Democracy of Knowledge"). The Quintuple Helix extends the Quadruple Helix by aspects of the "natural environments of society and economy," "social ecology," and the "socio-ecological transition." Also this environmental context of society can be better addressed in a democracy than in a nondemocracy. The current world appears to be challenged by a race between developing democracies versus emerging autocracies over knowledge production and innovation.

Keywords

Coevolution · Cross-Employment and Multiemployment · Cyber-Development, Democracy of Knowledge · Democracy, Knowledge Production, and Innovation · Society-Nature Interactions · Socioecological Transition · Multilevel Innovation Systems · Innovation Ecosystem · Twenty-First Century Fractal Research and Education and Innovation Ecosystem (FREIE) · Networks and Network Governance · Linear and Nonlinear Innovation · Quadruple Helix Innovation Systems · Quadruple Helix Plus · Quintuple Helix

Introduction

The concept of Triple Helix innovation systems was introduced by Etzkowitz and Leydesdorff (for example, see Etzkowitz and Leydesdorff 2000). The metaphor of *Helix* or *Helixes* (*Helices, spirals*) refers here to interwoven and cross-connected and cross-interconnected sectors. Triple Helix is possible within a democracy. However, Triple Helix is also possible without a democracy. The Triple Helix focuses on the knowledge economy, which may be approached by a democratic or a nondemocratic political framework. Nondemocratic (authoritarian) political regimes may be tempted to implement varieties of Triple Helix designs. Per definition, to already begin with a conceptual starting point, it is impossible for a nondemocratic

(authoritarian) political regime to try to implement a Quadruple Helix (Carayannis and Campbell 2012). *There is no Quadruple Helix without democracy* (Campbell and Carayannis 2013a, 2015; Campbell et al. 2015). In addition, evidence suggests that the ecological sensitivity of the Quintuple Helix (Carayannis et al. 2012) can be more easily or realistically be implemented and promoted within a democratic context of knowledge production and innovation. For the Quadruple Helix the "democracy matters": *this is in line with a view of a "Neo-Renaissance" where democracy encourages development in action for smart, sustainable, and inclusive growth, by this advocating sustainable development.* This should allow for "happy accidents" (Carayannis et al. 2016). For discourses on knowledge and innovation, a *Democracy* versus *Technocracy* issue can be postulated, where technocratic (and bureaucratic) approaches to innovation in nondemocratic regimes are being questioned and challenged by knowledge production and innovation in democracies. Also for the developing countries and emerging markets this has implications and ramifications, where there should be expectations that developments in knowledge and innovation are paralleled by progress in democratization (of course, this may not be always the case in empirical terms or empirically). Democracy acts as one of the levers that "happy accidents" in knowledge production and innovation are being transformed and translated into opportunities and benefits for society and to the people. Can there also be a "democratic capitalism," and which attempts of realization can there be approached or tried out (Carayannis and Kaloudis 2010)?

Definition of Key Terms: Innovation, Knowledge Production, Democracy, and Governance

The term or concept of innovation can have several meanings. Innovation may mean "change" only or can also refer to an "improvement" or "betterment." In a modern or more recent sense, innovation is being understood mostly as knowledge-based or knowledge-driven. So how can there be a change, improvement, betterment, or reform, which is leveraging, using, and applying knowledge? While knowledge production (or knowledge creation) is often associated closer to research (R&D), innovation expresses a focus of utilizing knowledge for economic (economy), social (society), and political (democracy) purposes. In that sense, mature innovation and innovation systems require a knowledge base or knowledge production.

Bengt-Åke Lundvall paraphrased Boulding (1985) by saying that a system could be seen as the opposite to chaos. In more detail, Lundvall (1992, p. 2) says: "Somewhat more specifically, a system is constituted by a number of elements and by the relationships between these elements." In the words of Kuhlmann (2001, p. 955), a system is: "As a system we understand a conglomeration of actors, institutions and processes all functionally bound together, whereby certain characteristic core functions of each form the demarcation criteria against other societal (sub)systems." In the process of a definition of a system, often two aspects are coming together: the elements of a system and the self-rational of a system. With the logic of this particular approach, the following definition can be offered for a system:

"1. *Elements:* systems consist of elements (parts); 2. *Self-Rationale:* systems have a mode of operation, a self-rationale (logic, self-logic), which organizes the self-organization and reproduction of a system and the relationship between the elements within a system and, furthermore, the relationship between the system and the other systems" (Carayannis et al. 2016, p. 4; Campbell 2001, p. 426).

In innovation theory, networks and clusters are important. "Innovation networks" and "knowledge clusters" (Carayannis and Campbell 2006) introduce here new perspectives. Networks underscore the importance of boundary-transcending interlinking and interlinkages in interdisciplinary, transdisciplinary, and transsectoral formats. The concept of sectoral systems of innovation (Malerba 1999, 2002, 2004) also relates to ideas of clusters and networks. *Smart cities or knowledge cities represent another example for knowledge clusters.* This puts forward the demand and requirement to conceptually bridge (or to "bride" in a metaphorical sense) networks and clusters *with* systems (and systems theory), leading to something like *networks of innovation networks and knowledge clusters:* "One way to look at this, is: clusters could be interpreted as an equivalent for the elements of a system; and networks as a (partial) equivalent for the relationship between the elements of one or of several systems. Networks may represent a specific, but crucial, subset of relations, relationships. *Through networking the clusters/elements of a system (of different systems) relate and interact (and communicate)*" (Carayannis et al. 2016, p. 8). Is a system being embedded by a larger system, then this system qualifies to be interpreted as a cluster or an element of a larger meta-system. Furthermore, elements or clusters within a system could be tested if they also qualify to be considered being a subsystem (or micro-system). This clearly expresses *fractal characteristics* in structure and process.

In a *spatial approach*, the multilevel system approach can address different layers, such as global, supranational, national, regional, and local. The national system of innovation represents here one of the core understandings. Bengt-Åke Lundvall (1992, p. 2) defines the national innovation system in the following way: "It follows that a system of innovation is constituted by elements and relationships which interact in the production, diffusion and use of new, and economically useful, knowledge and that a national system encompasses elements and relationships, either located within or rooted inside the borders of a nation state . . . it is obvious that the national system of innovation is a *social* system. A central activity in the system of innovation is learning, and learning is a social activity, which involves interaction between people." In this regard, Lundvall (1992, p. 4) depicted the modern Western nation states as "engines of growth." Also Richard R. Nelson (1990, p. 193) sees capitalism as an "engine of progress". But despite this focus on the national level, Lundvall was from the beginning explicit, by acknowledging the global and also the regional levels and dimensions of innovation. "Both globalisation and regionalisation might be interpreted as processes which weaken the coherence and importance of national systems" (Lundvall 1992, p. 3). So, by this, it could be argued that Lundvall had framed his ideas of a national innovation system already from the beginning within the context of multilevel architectures, meaning it does not make sense to talk about a national level without acknowledging global

and (subnational) regional and local levels. What Lundvall said is that the national level does matter, because it exists. Similarly argues Stefan Kuhlmann. He could be interpreted in a way of suggesting a possible coevolution between political systems and innovation systems. "Interwoven national and transnational governance mechanisms may feed the development of a transnational political system, including and building upon transformed national systems, fulfilling both 'local' (i.e. regional or national) and 'supra-local' functions at the same time" (Kuhlmann 2001, p. 956). Also Kuhlmann (2001, p. 954) sees the national level of an innovation system being accompanied in parallel by regional innovation systems: "In the meantime, national and increasingly also regional governments of all these countries pursue, more or less explicitly, 'innovation policies', understood here as the integral of all state initiatives regarding science, education, research, technology policy and industrial modernization, overlapping also with industrial, environmental, labour and social policies."

In that sense, there is also always a momentum of coevolution between the (multilevel) innovation system and the (multilevel) political system.

A *democracy* can be regarded as a system that refers to four underlying conceptual dimensions: freedom, equality, control, and sustainable development. "In theoretical and conceptual terms, we refer to a Quadruple-Dimensional structure, also a Quadruple Helix structure (a 'Model of Quadruple Helix Structures') of the four basic (conceptual) dimensions of freedom, equality, control, and sustainable development for explaining and comparing democracy and quality of democracy" (Campbell et al. 2015, p. 467). "There is a potential that democracy discourses and innovation discourses advance in a next-step and two-way mutual cross-reference. The architectures of Quadruple Helix (and Quintuple Helix) innovation systems demand and require the formation of a democracy, implicating that quality of democracy provides for a support and encouragement of innovation and innovation systems, so that quality of democracy and progress of innovation mutually 'Cross-Helix' in a connecting and amplifying mode and manner. This relates research on quality of democracy to research on innovation (innovation systems) and the knowledge economy" (Campbell et al. 2015, p. 468). In a more narrow understanding, a democracy falls together with a "democratic" political system. In a broader understanding, a democracy includes a democratic political system but extends also to the relevant contextualization of the political system. Further attributes of a democracy are pluralism, heterogeneity, and diversity.

The argument here is not that authoritarian (semi-authoritarian) political systems cannot develop a national innovation system. However, the argument is that authoritarian (semi-authoritarian) political systems are not in a position to advance (or to transform) a national innovation system to next higher levels of maturity. Particularly for Russia and China this is of relevance and will be of further interest in the coming years.

The term and concept of *governance* may be defined as processes of organization or self-organization of different systems, for example, the political, economic, or innovation systems. Governance utilizes strategies and policies in theory and practice.

Innovation Systems in Conceptual Evolution: Mode 3 Knowledge Production in Quadruple and Quintuple Helix Innovation Systems

Triple Helix Innovation Systems and Mode 1 and Mode 2 of Knowledge Production

Universities, or higher education institutions (HEIs) in more general, have three main functions: teaching and education, research (research and experimental development, R&D), and the so-called third mission activities, for example, innovation (Campbell and Carayannis 2013b, p. 5). In reference to "arts universities," now the question and challenge arises, whether, to which extent and in which way the arts universities differ from the (more traditional) universities in the sciences. Arts universities obviously place an emphasis on the arts, and the arts are not identical with the sciences. However, also arts universities frequently make references to the sciences, thus also arts universities can express competences in teaching and in carrying out research in the sciences. *The other major challenge of arts universities is to engage in "artistic research" and "arts-based innovation." By this, arts universities (and other higher education institutions in the arts) are also being linked to and are being interlinked with national innovation systems and multilevel innovation systems.* This widens the whole interdisciplinary and transdisciplinary spectrum of higher education systems. *"Artistic research" furthermore complements the "teaching of arts" at arts universities* (see also the propositions formulated by Bast 2013). Hybrid and innovative combinations of universities of arts and universities of the sciences are possible and indicate organizational opportunities for promoting creativity (Campbell 2013b).

University research, in a traditional understanding and in reference to universities in the sciences, focuses on basic research, often framed within a matrix of academic disciplines, and without a particular interest in the practical use of knowledge and innovation. This model of university-based knowledge production also is being called "Mode 1" of *knowledge production* (Gibbons et al. 1994). Mode 1 is also compatible with the linear model of innovation, which is often being referred to Vannevar Bush (1945). The linear model of innovation asserts that first there is basic research in university context: gradually, this university research will diffuse out into society and the economy. It is then the economy and the firms that pick up the lines of university research, and develop these further into knowledge application and innovation, for the purpose of creating economic and commercial success in the markets outside of the higher education system. Within the frame of linear innovation, there is a sequential "first-then" relationship between basic research (knowledge production) and innovation (knowledge application).

The Mode-1-based understanding of knowledge production has been challenged by the new concept of "Mode 2" of knowledge production, which was developed and proposed by Michael Gibbons et al. (1994, pp. 3–8, 167). Mode 2 emphasizes a knowledge application and a knowledge-based problem-solving that involves and encourages the following principles: "knowledge produced in the context of application"; "transdisciplinarity"; "heterogeneity and organizational diversity"; "social

accountability and reflexivity"; and "quality control" (see furthermore Nowotny et al. 2001, 2003, 2006). Key in this setting is the focus on a knowledge production in contexts of application. Mode 2 expresses and encourages clear references to innovation and innovation models. The linear model of innovation also has become challenged by nonlinear models of innovation, which are interested in drawing more direct connections between knowledge production and knowledge application, where basic research and innovation are being coupled together not in a first-then but in an "as well as" and "parallel" (parallelized) relationship (Campbell and Carayannis 2012). Mode 2 appears also to be compatible with nonlinear innovation and its ramifications.

The Triple Helix model of knowledge, innovation, and university-industry-government relations, which was introduced and developed by Henry Etzkowitz and Loet Leydesdorff (2000, pp. 111–112), asserts a basic core model for knowledge production and innovation, where three "helices" intertwine, by this creating a national innovation system. The three helices are identified by the following systems or sectors: academia (universities), industry (business), and state (government). In the current innovation discourses, the "Triple Helix" model represents something like a "standard model" of (and for) innovation (by this being something like a "null hypothesis"). Etzkowitz and Leydesdorff refer to "university-industry-government relations" and networks, putting a particular emphasis on "tri-lateral networks and hybrid organizations," where those helices overlap in a hybrid fashion. Etzkowitz and Leydesdorff (2000, p. 118) also explain, how, in their view, the Triple Helix model relates to Mode 2: the "Triple Helix overlay provides a model at the level of social structure for the explanation of Mode 2 as an historically emerging structure for the production of scientific knowledge, and its relation to Mode 1". More recently, Leydesdorff (2012) also introduced the notion of "N-Tuple of Helices" (Park 2014).

Quadruple and Quintuple Helix Innovation Systems and Mode 3 of Knowledge Production

Mode 1 and Mode 2 may be characterized as "knowledge paradigms" that underlie the knowledge production (to a certain extent also the knowledge application) of higher education institutions and university systems. Success or quality, in accordance with Mode 1, may be defined as: "*academic excellence, which is a comprehensive explanation of the world (and of society) on the basis of 'basic principles' or 'first principles', as is being judged by knowledge producer communities (academic communities structured according to a disciplinary framed peer review system).*" Consequently, success and quality, in accordance with Mode 2, can be defined as: "*problem-solving, which is a useful (efficient, effective) problem-solving for the world (and for society), as is being judged by knowledge producer and knowledge user communities*" (Campbell and Carayannis 2013b, p. 32; see furthermore Campbell and Carayannis 2013c, 2016a). A "Mode 3" university, higher education institution or higher education system would represent a type of organization or

system that seeks creative ways of combining and integrating different principles of knowledge production and knowledge application (for example, Mode 1 and Mode 2), by this encouraging diversity and heterogeneity and also creating creative and innovative organizational contexts for research and innovation (Carayannis and Campbell 2006; Carayannis et al. 2016). Mode 3 encourages the formation of "creative knowledge environments" (Hemlin et al. 2004). "Mode 3 universities," Mode 3 higher education institutions and systems, are prepared to perform "basic research in the context of application" (Campbell and Carayannis 2013b, p. 34). This has furthermore qualities of nonlinear innovation. Governance of higher education and governance in higher education must also be sensitive, whether a higher education institution operates on the basis of Mode 1, Mode 2, or a combination of these in Mode 3. The concept of "epistemic governance" emphasizes that the underlying knowledge paradigms of knowledge production and knowledge application are being addressed by quality assurance and quality enhancement strategies, policies, and measures (Campbell and Carayannis 2013b, c).

Emphasizing again a more systemic perspective for the Mode 3 knowledge production, a focused conceptual definition may be as follows (Carayannis and Campbell 2012, p. 49): Mode 3 "... allows and emphasizes the co-existence and co-evolution of different knowledge and innovation paradigms. In fact, a key hypothesis is: *The competitiveness and superiority of a knowledge system or the degree of advanced development of a knowledge system are highly determined by their adaptive capacity to combine and integrate different knowledge and innovation modes* via *co-evolution, co-specialization and co-opetition knowledge stock and flow dynamics*" (see Carayannis and Campbell 2009; on "Co-Opetition," see Brandenburger and Nalebuff 1997). Analogies are being drawn and a coevolution is being suggested between diversity and heterogeneity in advanced knowledge society and knowledge economy, and political pluralism in democracy (knowledge democracy), and the quality of a democracy. The "Democracy of Knowledge" refers to this overlapping relationship. As is being asserted: "The *Democracy of Knowledge*, as a concept and metaphor, highlights and underscores parallel processes between political pluralism in advanced democracy, and knowledge and innovation heterogeneity and diversity in advanced economy and society. Here, we may observe a hybrid overlapping between the *knowledge economy, knowledge society and knowledge democracy*" (Carayannis and Campbell 2012, p. 55). The "Democracy of Knowledge," therefore, is further-reaching than the earlier idea of the "Republic of Science" (Michael Polanyi 1962). This is because there can be a republic that is not democratic: but there cannot be a democracy that is not a democracy (to put forward here a statement in metaphorical terms).

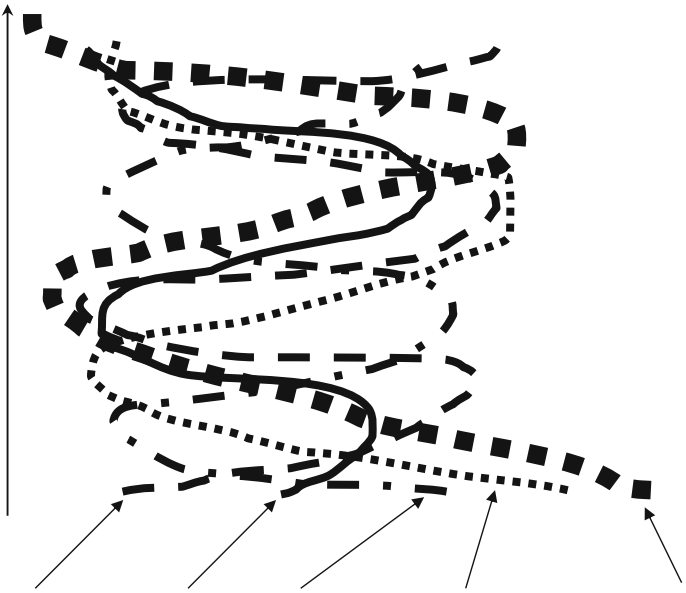
Democracy may be defined as a system that is based on the following principles: freedom, equality, control, and sustainable development (Campbell et al. 2015). We postulated a coevolution between political systems and innovation systems. Therefore, in this understanding, innovation systems in democracies will differ from innovation systems in nondemocracies. Is there even an expectation of a certain *coevolution between knowledge economy and knowledge democracy*, this ultimately means that certain higher levels of innovation and innovation system are not possible

without a context of a democracy (Carayannis and Campbell 2014). Advanced knowledge economies and knowledge societies require knowledge and innovation pluralism, and this meets with political pluralism in advanced democracies.

The main focus of the Triple Helix innovation model concentrates on university-industry-government relations (Etzkowitz and Leydesdorff 2000). In that respect, Triple Helix represents a basic model or a core model for knowledge production and innovation application. The models of the Quadruple Helix and Quintuple Helix innovation systems are designed to comprehend already and to refer to an extended complexity in knowledge production and knowledge application (innovation), thus, the analytical architecture of these models is broader conceptualized. To use metaphoric terms, the Quadruple Helix embeds and contextualizes the Triple Helix, while the Quintuple Helix embeds and contextualizes the Quadruple Helix (and Triple Helix). The Quadruple Helix adds as a fourth helix the "media-based and culture-based public," the "civil society," and "arts, artistic research and arts-based innovation" (Carayannis and Campbell 2009, 2012, p. 14; Carayannis and Pirzadeh 2014; Campbell and Carayannis 2016b; see also: Bast et al. 2015; Danilda et al. 2009; Eigelsreiter 2017; Hemlin et al. 2004; Mitterlehner 2014). *The Quadruple Helix also could be emphasized as the perspective that specifically brings in the "dimension of democracy" or the "context of democracy" for knowledge, knowledge production, and innovation.* The Quintuple Helix innovation model even is more comprehensive in its analytical and explanatory stretch and approach, adding furthermore the fifth helix (and perspective) of the "natural environments of society" (Carayannis and Campbell 2010, p. 62) (see Figs. 1 and 2).

The introduction of the arts has here two implications: (1) The arts act as a source of creativity, which qualifies as a further necessary input to advance innovation. (2) The different disciplines of the arts extend the established disciplines in the sciences, social sciences, and humanities, and by this promote an extended understanding and new and innovative formats of interdisciplinarity but also transdisciplinarity.

The Triple Helix is explicit in acknowledging the importance of higher education for innovation. However, it could be argued that the Triple Helix sees knowledge production and innovation in relation to economy, thus the Triple Helix models first of all (primarily) the economy and economic activity. In that sense, the Triple Helix frames the knowledge economy. The Quadruple Helix brings in the additional perspective of society (knowledge society) and of democracy (knowledge democracy). The Quadruple-Helix-innovation-system understanding emphasizes that sustainable development of and in economy (knowledge economy) requires that there is a coevolution of knowledge economy and knowledge society and knowledge democracy. The Quadruple Helix even encourages *the perspectives of knowledge society and of knowledge democracy* for supporting, promoting, and advancing knowledge production (research) and knowledge application (innovation). Furthermore, the Quadruple Helix is also explicit that not only universities (higher education institutions) of the sciences but also universities (higher education institutions) of the arts should be regarded as decisive and determining institutions for advancing next-stage innovation systems: the interdisciplinary and transdisciplinary connection



First Helix: Academia / universtities	Second Helix: Industry / business	Third Helix: State / government	Fourth Helix: Media-based and culture-based public; civil society; arts, artistic reseach and arts-based innovation /	Fifth Helix: Natural environment, natural environments of society and economy /
Universities (higher education institutions) of the sciences and of the arts.	Also: creativity economy and creative industries.		culture and innovation culture, knowledge of culture and culture of knowledge, values and life styles, multi-culturalism and creativity, media, arts and arts universities, multi-level innovation systems with universities of the sciences and arts.	social ecology, society-nature interactions, socio-ecological transition.

Triple Helix:	**University-industry-government relations (helices).**
Quadruple Helix, Fourth Helix:	**"Media-based and culture-based public", "civil society" and "arts, artistic research and arts-based innovation" (helix).**
Quintuple Helix, Fifth Helix:	**Natural envrionment, natural environments of society and economy (helix).**

Fig. 1 The Quadruple and Quintuple Helix innovation systems (Source: Authors' own conceptualization based on Etzkowitz and Leydesdorff (2000, p. 112), Carayannis and Campbell (2009, p. 207, 2012, p. 14, 2013) and Danilda et al. (2009))

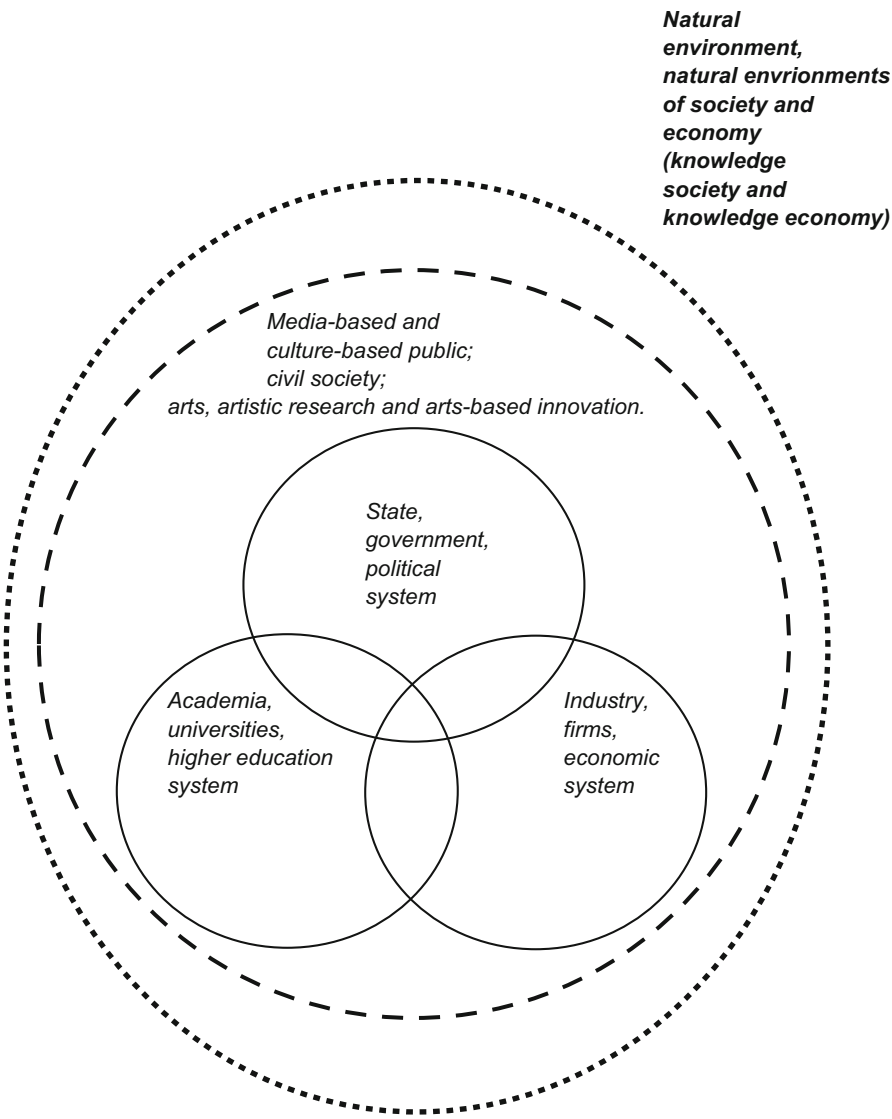


Fig. 2 The Quintuple Helix (five-helix model) innovation system (Source: Authors' own conceptualization based on Carayannis and Campbell (2010, p. 62))

of sciences and arts creates crucial and creative combinations for promoting and supporting innovation. Here, in fact, lies one of the keys for future success. The concept and term of "social ecology" refers to "society-nature interactions" between "human society" and the "material world" (see, for example, Fischer-Kowalski and

Haberl 2007). The European Commission (2009) identified the necessary socio-ecological transition of economy and society as one of the great next-phase challenges, but also as an opportunity, for the further progress and advancement of knowledge economy and knowledge society. The Quintuple Helix refers to this socioecological transition of society, economy, and democracy; the Quintuple Helix innovation system is therefore ecologically sensitive. Quintuple Helix bases its understanding of knowledge production (research) and knowledge application (innovation) on social ecology (see Fig. 3). Environmental issues (such as global

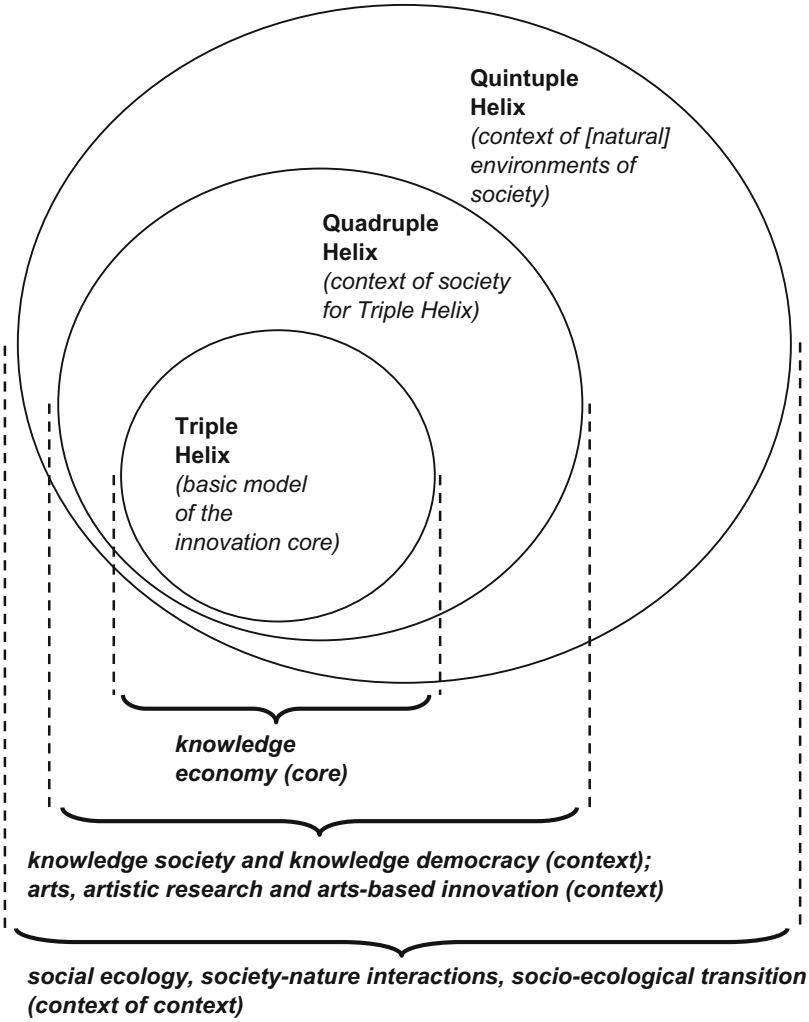


Fig. 3 The Quadruple and Quintuple Helix innovation systems in relation to society, economy, democracy, and social ecology (Source: Authors' own conceptualization based on Carayannis et al. (2012, p. 4))

warming) represent issues of concern and of survival for humanity and human civilization. But the Quintuple Helix translates environmental and ecological issues of concern also in potential opportunities, by identifying them as possible drivers for future knowledge production and innovation (Carayannis et al. 2012). This, finally, defines also opportunities for the knowledge economy. "*The Quintuple Helix supports here the formation of a win-win situation between ecology, knowledge and innovation, creating synergies between economy, society and democracy*" (Carayannis et al. 2012, p. 1).

Conclusion

The terms and concepts of Mode 3 knowledge production and Quadruple Helix innovation systems were first introduced to international academic debate by Carayannis and Campbell (2006, 2009) and were later developed further (Carayannis and Campbell 2012). The same applies to the Quintuple Helix (Carayannis and Campbell 2010). From the beginning, the "media-based and culture-based public" as well as universities and other higher education institutions of the arts were being regarded as crucial attributes and components of the Quadruple and Quintuple Helix innovation systems, *implying that arts are essential for the progress and evolution of innovation systems* (see again Figs. 1 and 2). *In our analysis here, we developed more specifically the Quadruple and Quintuple Helix innovation systems in terms and in favor of arts, artistic research, and arts-based innovation. We wanted to demonstrate the full momentum and flexibility of the Quadruple and Quintuple Helix for conceptually addressing and integrating art and arts*.

In the future, what are further challenges for innovation systems? Which issues should be addressed for the design, design evolution, and governance of (and within) innovation systems? More generally speaking, further ramifications of Mode 3 knowledge production in Quadruple Helix and Quintuple Helix innovation systems are:

1. *Multilevel innovation systems, the global and the local (GloCal):* Lundvall was pivotal for introducing the concept of the "national innovation system." Lundvall (1992, pp. 1, 3) explicitly acknowledges that national innovation systems are challenged in permanence (but are also extended) by regional as well as global innovation systems. Here, Kuhlmann (2001, pp. 960–961) could be paraphrased and the assertion that as long as nation-states and nation state-based political systems exist, it is plausible to use the concept of the national innovation system. More comprehensive in its analytical architecture than the national innovation system is the concept of the "multi-level innovation system" (Carayannis and Campbell 2012, pp. 32–35). In a spatial understanding, multilevel innovation systems compare the national not only with the subnational (regional, local) but also with the transnational and global levels (see, for example, Kaiser and Prange

2004; furthermore, see Pfeffer 2012, and Merz and Sormani 2016). However, it is also important to extend multilevel innovation systems to the challenges and potential benefits and opportunities of a nonspatial meaning, understanding, and "mapping": "Therefore, multi-level systems of knowledge as well as multi-level systems of innovation are based on spatial and non-spatial axes. A further advantage of this multi-level systems architecture is that it results in a more accurate and closer-to-reality description of processes of globalization and *gloCalization*" (Carayannis and Campbell 2012, p. 35).

2. *Linear and nonlinear innovation:* Knowledge application and innovation are being challenged and driven out of an interest of combining and integrating linear and nonlinear innovation. Key here are diversity, heterogeneity, and pluralism of different knowledge and innovation modes and their linking-together via an architecture of coevolving networks. Firms, universities, and other organizations can engage (at the same) in varying and multiple technology life cycles at different levels of maturity. Another way, how to think nonlinear innovation, is being suggested by the concept of cross-employment (Campbell 2011, 2013a). As a form and type of multiemployment, cross-employment emphasizes that the same individual may be employed by two (or more) organizations at the same time, where one organization could be located closer to knowledge production and the other to knowledge application (innovation): are those organizations also rooted in different sectors, then cross-employment acts also as a transsectoral networking (Campbell and Caraynnis 2013b, pp. 65, 68). *Cross-employment can furthermore bridge different sectors and disciplines in the sciences with different disciplines in the arts.* What results is a "Mode 3 Innovation Ecosystem": "This parallel as well as sequentially time-lagged unfolding of technology life cycles also expresses characteristics of Mode 2 and of nonlinear innovation, because organizations (firms and universities) often must develop strategies of simultaneously cross-linking different technology life cycles. Universities and firms (commercial and academic firms) must balance the nontriviality of a fluid pluralism of technology life cycles" (Carayannis and Campbell 2012, p. 37; see furthermore Dubinaet al. 2012). The "academic firm" (Campbell and Carayannis 2016b) may also be compared with attributes of the so-called network firm (Laperche and Uzunidis 2018). The relationship between networks, "cooperation and competition" ("Co-Opetition"), represents a challenge and sensitive issue and allows for different creative answers in organizational representation and manifestation.
3. *Twenty-first century Fractal Research, Education and Innovation Ecosystem (FREIE):* Here, the understanding of FREIE is: "This is *a multilayered*, *multimodal*, *multinodal, and multilateral system*, encompassing mutually complementary and reinforcing innovation networks and knowledge clusters consisting of human and intellectual capital, shaped by social capital and underpinned by financial capital" (Carayannis and Campbell 2012, p. 3).
4. *Linear and nonlinear innovation, and the causality of "if-then" and of "if-if" relations:* The hybrid overlapping of linear innovation and of nonlinear

> innovation displays also possible ramifications and draws associations to models of causality and their remodeling. "We can speculate, whether this parallel integration of linearity and nonlinearity not also encourages a new approach of paralleling in our theorizing and viewing of causality: *in epistemic (epistemological) terms, the so-called if-then relationships could be complemented by (a thinking in) 'if-if' relations*" (Carayannis and Campbell 2012, p. 24).

The Quadruple Helix regards itself to be "human-center" oriented. While for the Triple Helix model the existence of a democracy is not (per se) necessary for knowledge production and innovation, the Quadruple Helix is here more explicit. The way, how the Quadruple Helix is being engineered, designed, and "architected," from that it is clear that there cannot be a Quadruple Helix innovation system without democracy or a democratic context. The following attributes and components define the fourth helix in the Quadruple Helix: "media-based and culture-based public," "civil society," and "arts, artistic research and arts-based innovation." By this the fourth helix in the Quadruple Helix represents the perspective of the "dimension of democracy" or the "context of democracy" for knowledge, knowledge production, and innovation. This is particularly true when democracy is being understood to transcend the narrow understanding of being primarily based *on* or being primarily rooted *in* government institutions (within Triple Helix). Civil society, culture-based public, quality of democracy, and sustainable development convincingly demonstrate what the rationales and requirements are for conceptualizing democracy broader (Campbell and Carayannis 2013a). To turn this line of thinking: autocracies are not interested to allow the development of a free and mature civil society. On the contrary, autocracies want to control and suppress the rise of an independent civil society. *Political pluralism in a democracy coevolves with the pluralism, diversity, and heterogeneity of knowledge, knowledge production, and innovation* ("Democracy of Knowledge," see Carayannis and Campbell 2009, 2012, p. 55). *We postulate here a congruence of structures and processes in democracy and in innovation systems*. The Quintuple Helix extends the Quadruple Helix by aspects of the "natural environments of society and economy," "social ecology," and the "socio-ecological transition." Also, this environmental context of society can be better addressed in a democracy than in a nondemocracy. *The current world appears to be challenged by a race between developing democracies* versus *emerging autocracies over knowledge production and innovation*.

Cyber-Development can be defined as a development in terms of a sustainable development of knowledge economy, knowledge society, and knowledge democracy that is knowledge-based and knowledge-driven, and where innovation is playing a crucial role. In this understanding, the Quadruple and Quintuple Helix innovation systems provide a model and conceptual framework for theory and practice, strategy and policy for progress and advancement exactly in knowledge economy, knowledge society, and knowledge democracy. This introduces new perspectives for a new type of governance and a new set of policies for problem-solving and further evolution.

Cross-References

- ▶ Academic Firm in Cyber-Development: The New Design and Redesign Proposition for Entrepreneurship in the Innovation-Driven Knowledge Economy
- ▶ Epistemic Governance and Epistemic Innovation Policy in Higher Education for Cyber-Development
- ▶ Quality of Democracy in Quadruple Helix Structures: OECD Countries in Global Comparison

References

Bast, G. (2013). Preparing a "creative revolution" – Arts and universities of the arts in the creative knowledge economy. In E. G. Carayannis (Editor-in-Chief), I. N. Dubina, N. Seel, D. F. J. Campbell, & D. Uzunidis (Associate Editors) (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 1471–1476). New York: Springer. http://link.springer.com/referenceworkentry/10.1007/978-1-4614-3858-8_442

Bast, G., Carayannis, E. G., & Campbell, D. F. J. (Eds.). (2015). *Arts, research, innovation and society*. New York: Springer. http://www.springer.com/business+%26+management/technology+management/book/978-3-319-09908-8

Boulding, K. E. (1985). *The world as a total system*. Beverly Hills: Sage.

Brandenburger, A. M., & Nalebuff, B. J. (1997). *Co-opetition*. New York: Doubleday.

Bush, V. (1945). *Science: The endless frontier*. Washington, DC: United States Government Printing Office. http://www.nsf.gov/od/lpa/nsf50/vbush1945.htm#transmittal

Campbell, D. F. J. (2001). Politische Steuerung über öffentliche Förderung universitärer Forschung? Systemtheoretische Überlegungen zu Forschungs- und Technologiepolitik. [Political steering through public support of university research? Systems-theoretical considerations about research and technology policy]. *Österreichische Zeitschrift für Politikwissenschaft (Austrian Journal of Political Science), 30*(4), 425–438.

Campbell, D. F. J. (2011). Wissenschaftliche „Parallelkarrieren" als Chance. Wenn Wissenschaft immer öfter zur Halbtagsbeschäftigung wird, könnte eine Lösung im „Cross-Employment" liegen. Guest Commentary for DIE PRESSE February 2, 2011. http://diepresse.com/home/bildung/meinung/635781/Wissenschaftliche-Parallelkarrieren-als-Chance?direct=635777&_vl_backlink=/home/bildung/index.do&selChannel=500

Campbell, D. F. J. (2013a). Cross-employment. In E. G. Carayannis (Editor-in-Chief), I. N. Dubina, N. Seel, D. F. J. Campbell, & D. Uzunidis (Associate Editors) (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 503–508). New York: Springer. http://link.springer.com/referenceworkentry/10.1007/978-1-4614-3858-8_254

Campbell, G. S. (2013b). Speaking pictures: Innovation in fine arts. In E. G. Carayannis (Editor-in-Chief), I. N. Dubina, N. Seel, D. F. J. Campbell, & D. Uzunidis (Associate Editors) (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 1716–1722). New York: Springer. http://link.springer.com/referenceworkentry/10.1007/978-1-4614-3858-8_484

Campbell, D. F. J., & Carayannis, E. G. (2012). Lineare und nicht-lineare knowledge production: Innovative Herausforderungen für das Hochschulsystem. *Zeitschrift für Hochschulentwicklung, 7*(2), 64–72. http://www.zfhe.at/index.php/zfhe/article/view/448

Campbell, D. F. J., & Carayannis, E. G. (2013a). Quality of democracy and innovation. In E. G. Carayannis (Editor-in-Chief), I. N. Dubina, N. Seel, D. F. J. Campbell, & D. Uzunidis (Associate Editors) (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 1527–1534). New York: Springer. http://link.springer.com/referenceworkentry/10.1007%2F978-1-4614-3858-8_509#

Campbell, D. F. J., & Carayannis, E. G. (2013b). *Epistemic governance in higher education. Quality enhancement of universities for development. SpringerBriefs in business*. New York: Springer. http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6

Campbell, D. F. J., & Carayannis, E. G. (2013c). Epistemic governance and epistemic innovation policy. In E. G. Carayannis (Editor-in-Chief), I. N. Dubina, N. Seel, D. F. J. Campbell, & D. Uzunidis (Associate Editors) (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 697–702). New York: Springer. http://link.springer.com/referenceworkentry/10.1007/978-1-4614-3858-8_271

Campbell, D. F. J., & Carayannis, E. G. (2015). Explaining and comparing quality of democracy in quadruple helix structures: The quality of democracy in the United States and in Austria, challenges and opportunities for development. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice*. New York: Springer. http://www.springer.com/social+sciences/political+science/book/978-1-4939-1027-4

Campbell, D. F. J., & Carayannis, E. G. (2016a). Epistemic governance and epistemic innovation policy. *Technology, Innovation and Education, 2*(2), 1–15. https://doi.org/10.1186/s40660-016-0008-2. http://technology-innovation-education.springeropen.com/articles/10.1186/s40660-016-0008-2

Campbell, D. F. J., & Carayannis, E. G. (2016b). The academic firm: A new design and redesign proposition for entrepreneurship in innovation-driven knowledge economy. *Journal of Innovation and Entrepreneurship, 5*(12), 1–10. https://doi.org/10.1186/s13731-016-0040-1. http://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-016-0040-1

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493. http://link.springer.com/article/10.1007/s13132-015-0246-7

Carayannis, E. G., & Campbell, D. F. J. (2006). Mode 3″: Meaning and implications from a knowledge systems perspective. In E. G. Carayannis & D. F. J. Campbell (Eds.), *Knowledge creation, diffusion, and use in innovation networks and knowledge clusters. A comparative systems approach across the United States, Europe and Asia* (pp. 1–25). Westport: Praeger.

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "Quadruple Helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46*(3/4), 201–234. http://www.inderscience.com/browse/index.php?journalID=27&year=2009&vol=46&issue=3/4 and http://www.inderscience.com/search/index.php?action=record&rec_id=23374&prevQuery=&ps=10&m=or

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69. https://www.igi-global.com/article/triple-helix-quadruple-helix-quintuple/41959

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development. SpringerBriefs in business*. New York: Springer. http://www.springer.com/business+%26+management/book/978-1-4614-2061-3

Carayannis, E. G., & Campbell, D. F. J. (2014). Developed democracies versus emerging autocracies: Arts, democracy, and innovation in quadruple helix innovation systems. *Journal of Innovation and Entrepreneurship, 3*(12), 1–23. http://www.innovation-entrepreneurship.com/content/3/1/12

Carayannis, E. G., & Kaloudis, A. (2010). A time for action and a time to lead: Democratic capitalism and a new "New Deal" for the US and the world in the twenty-first century. *Journal of the Knowledge Economy, 1*(1), 4–17. http://link.springer.com/article/10.1007/s13132-009-0002-y

Carayannis, E. G., & Pirzadeh, A. (2014). *The knowledge of culture and the culture of knowledge. implications for theory, policy and practice*. Houndmills: Palgrave Macmillan. http://www.

amazon.de/The-Knowledge-Culture-Implications-Practice/dp/1403942439/ref=sr_1_1?ie=UTF8&qid=1403080044&sr=8-1&keywords=carayannis+knowledge+of+culture

Carayannis, E. G., Barth, T. D., & Campbell, D. F. J. (2012). The quintuple helix innovation model: Global warming as a challenge and driver for innovation. *Journal of Innovation and Entrepreneurship, 1*(1), 1–12. http://www.innovation-entrepreneurship.com/content/pdf/2192-5372-1-2.pdf

Carayannis, E. G., Campbell, D. F. J., & Rehman, S. S. (2016). Mode 3 knowledge production: Systems and systems theory, clusters and networks. *Journal of Innovation and Entrepreneurship, 5*(17), 1–24. https://doi.org/10.1186/s13731-016-0045-9. http://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-016-0045-9

Danilda, I., Lindberg, M., & Torstensson, B. -M. (2009). Women resource centres. A quattro helix innovation system on the European agenda. Paper http://www.hss09.se/own_documents/Papers/3-11%20-%20Danilda%20Lindberg%20&%20Torstensson%20-%20paper.pdf

Dubina, I. N., Carayannis, E. G., & Campbell, D. F. J. (2012). Creativity economy and a crisis of the economy? Coevolution of knowledge, innovation, and creativity, and of the knowledge economy and knowledge society. *Journal of the Knowledge Economy, 3*(1), 1–24. http://link.springer.com/article/10.1007/s13132-011-0042-y

Eigelsreiter, B. (2017). Consumerization of IT, cyber-democracy and cyber-crime: The inherent challenges and opportunities of different ends of a continuum. In E. G. Carayannis, D. F. J. Campbell, M. P. Efthymiopoulos (Eds.), *Handbook of cyber-development, cyber-democracy, and cyber-defense*. New York: Springer. https://link.springer.com/referencework/10.1007%2F978-3-319-06091-0

Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation: From national systems and "mode 2" to a triple helix of university-industry-government relations. *Research Policy, 29*, 109–123.

European Commission. (2009). *The world in 2025. Rising Asia and socio-ecological transition*. Brussels: European Commission. http://ec.europa.eu/research/social-sciences/pdf/the-world-in-2025-report_en.pdf

Fischer-Kowalski, M., & Haberl, H. (Eds.). (2007). *Socioecological transitions and global change. Trajectories of social metabolism and land use*. Cheltenham: Edward Elgar.

Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P., & Trow, M. (Eds.). (1994). *The new production of knowledge. The dynamics of science and research in contemporary societies*. London: Sage.

Hemlin, S., Allwood, C. M., & Martin, B. R. (2004). *Creative knowledge environments. The influences on creativity in research and innovation*. Cheltenham: Edward Elgar.

Kaiser, R., & Prange, H. (2004). The reconfiguration of national innovation systems – The example of German biotechnology. *Research Policy, 33*, 395–408.

Kuhlmann, S. (2001). Future governance of innovation policy in Europe – Three scenarios. *Research Policy, 30*, 953–976.

Laperche, B., & Uzunidis, D. (2018). The knowledge capital of the network firm: Socialization versus business appropriation of scientific work. In G. Bast, E. G. Carayannis, & D. F. J. Campbell (rédacteurs) (Eds.), *The future of education and labor (ARIS series: Arts, research, innovation and society)*. New York: Springer (*forthcoming*).

Leydesdorff, L. (2012). The triple helix, quadruple helix, . . ., and an n-tuple of helices: Explanatory models for analyzing the knowledge-based economy? *Journal of the Knowledge Economy, 3*(1), 25–35. http://link.springer.com/article/10.1007/s13132-011-0049-4

Lundvall, B.-Å. (Ed.). (1992). *National systems of innovation. Towards a theory of innovation and interactive learning*. London: Pinter Publishers.

Malerba, F. (1999). Sectoral systems of innovation and production. DRUID conference on: National innovation systems, industrial dynamics and innovation policy (Rebild, June 9–12, 1999). http://www.druid.dk/uploads/tx_picturedb/ds1999-69.pdf

Malerba, F. (2002). Sectoral systems of innovation and production. *Research Policy, 31*(2), 247–264.

Malerba, F. (2004). *Sectoral systems of innovation: Concepts, issues and analyses of six major sectors in Europe*. Cambridge: Cambridge University Press.

Merz, M., & Sormani, P. (rédacteurs.). (2016). *The local configuration of new research fields. On regional and national diversity*. Cham: Springer.

Mitterlehner, B. (2014). Cyber-democracy and cybercrime: Two sides of the same coin, 207–230. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice*. New York: Springer.

Nelson, R. R. (1990). Capitalism as an engine of progress. *Research Policy, 19*, 193–214.

Nowotny, H., Scott, P., & Gibbons, M. (2001). *Re-thinking science. Knowledge and the public in an age of uncertainty*. Cambridge: Polity Press.

Nowotny, H., Scott, P., & Gibbons, M. (2003). Mode 2 revisited: The new production of knowledge. *Minerva, 41*, 179–194.

Nowotny, H., Scott, P., & Gibbons, M. (2006). Re-thinking science: Mode 2 in societal context. In E. G. Carayannis & D. F. J. Campbell (Eds.), *Knowledge creation, diffusion, and use in innovation networks and knowledge clusters. A comparative systems approach across the United States, Europe and Asia* (pp. 39–51). Westport: Praeger.

Park, H. W. (2014). Transition from the triple helix to N-tuple helices? An interview with Elias G. Carayannis and David F. J. Campbell. *Scientometrics, 99* (1), 203–207. http://link.springer.com/article/10.1007%2Fs11192-013-1124-3 and http://download.springer.com/static/pdf/907/art%253A10.1007%252Fs11192-013-1124-3.pdf?auth66=1397308723_4cb0003877af5305d5dc202280b9cd6d&ext=.pdf

Pfeffer, T. (2012). *Virtualization of universities. Digital media and the organization of higher education institutions*. New York: Springer. http://www.springer.com/business+%26+management/media+management/book/978-1-4614-2064-4

Polanyi, M. (1962). The republic of science: Its political and economic theory. *Minerva, 1*, 54–74. http://sciencepolicy.colorado.edu/students/envs_5100/polanyi_1967.pdf and http://fiesta.bren.ucsb.edu/~gsd/595e/docs/41.%20Polanyi_Republic_of_Science.pdf

Academic Firm in Cyber-Development: The New Design and Redesign Proposition for Entrepreneurship in the Innovation-Driven Knowledge Economy

3

David F. J. Campbell and Elias G. Carayannis

Contents

Abstract

The academic firm is a type of firm (firm-based organization or institution) that is being driven by focusing on encouraging, supporting, and advancing knowledge production (research, research and experimental development, R&D) and knowledge application (innovation). The academic firm interprets and qualifies a disciplinary (interdisciplinary) variety of the background of its employees (and

D. F. J. Campbell (✉)
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@aau.at; david.campbell@uni-ak.ac.at; david.campbell@univie.ac.at

E. G. Carayannis
Department of Information Systems and Technology Management, School of Business, The George Washington University, Washington, DC, USA
e-mail: caraye@gwu.edu

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_57

their competences) as a potential opportunity and asset to perform creatively in knowledge production and knowledge application. The academic firm has an interest to engage in networks with universities (higher education institutions) or other academic research institutions, driven out of a desire to access university knowledge (e.g., basic university research). In general, the academic firm values engagement in diversified networks as a form for creating knowledge as well as benefitting from opportunities. The academic firm accepts in principle, in certain situations even promotes, split employment or "cross-employment" (multi-employment) of its employees with other (academic) organizations or institutions, for example, universities or other higher education institutions. *The proposition here is that the academic firm represents a new design (and redesign) for entrepreneurship in innovation-driven knowledge economy.*

Keywords
Academic firm · Commercial firm · Creativity · Cross-employment · Cross-retirement · Cyber development · Design · Entrepreneurship · Innovation · Knowledge application · Knowledge economy · Knowledge production · Linear innovation · Networks · Nonlinear innovation · Redesign · Research (R&D)

Introduction

The "academic firm" represents a type of firm (firm-based organization) that focuses on encouraging, supporting, and advancing knowledge production (research, research and experimental development, R&D) and knowledge application (innovation). The academic firm is also inclined to generate profit (revenues) but follows here more the logic of a "sustainability" in balance with knowledge production and the principles of knowledge production. The contrary concept to the academic firm would be the "commercial firm," which is primarily being motivated and driven out of an interest of maximizing profit (revenues). Between these two conceptual poles of understanding, there are various possibilities of a gradual or also unconventional (radical) combination of principles for the empirical organization of a concrete firm, its organizational manifestation. The shortcut for a definition therefore is "The *Commercial Firm* concentrates on maximizing or optimizing profit, whereas the *Academic Firm* focuses on maximizing or optimizing knowledge and innovation" (Carayannis and Campbell 2012, p. 27).

Design and Redesign of the Academic Firm

Knowledge and innovation are crucial key drivers for the academic firm. Academic firms can follow the logic of linear innovation but also the logic of nonlinear innovation. The model of linear innovation often is being assigned to Vannevar Bush (1945). This model assumes a sequential "first-then" relationship, where there

is first basic research at universities that gradually diffuses out into society and economy and where firms then translate the lines of basic research into application and economic as well as commercial uses and profits. But nonlinear innovation favors a different approach. Nonlinear innovation is interested in a more direct and parallel coupling of knowledge production and knowledge application, where there are mutual interferences and parallel as well as parallelized interactions between basic research and knowledge application. The organization of nonlinear innovation encourages creative organizational designs (Campbell and Carayannis 2012). In the context of firm-based organizations, also for the academic firm, the processing and advancement of nonlinear innovation may imply (1) firms (academic firms) engage simultaneously in different technology life cycles at different levels of technology maturity and (2) firms (academic firms) accept to a certain extent, even encourage, cross-employment of their employees with other institutions, for example, academic institutions, such as universities or other higher education institutions. Cross-employment, as a concept, identifies forms and varieties of multi-employment, where an individual person is being simultaneously employed by more than one organization (by at least two organizations): should those organizations also root in different sectors, then cross-employment displays characteristics of a trans-sectoral network building (Campbell 2011).

Academic firms express a particular interest to network with universities, other higher education institutions, university-related institutions, and all forms and manifestations of organizations that conduct an academically based type of research or basic research. Academic firms explore also possibilities, options, and opportunities of networking with other firms (academic firms but also commercial firms). There always remains the challenge, how to balance and how to refer to each other (out of the perspective of the firms) with regard to cooperation and competition. Furthermore, networks can integrate aspects of cooperation and competition. The organizational design of patterns of cooperation and competition allows creativity and can also be captured and described by the notion and concept of "Co-Opetition" (Brandenburger and Nalebuff 1997) (see Fig. 1).

Knowledge production in the context of universities and the higher education system has been explained on the basis of the models of "Mode 1" and "Mode 2" of knowledge production. Mode 1 emphasizes a traditional understanding and refers to university basic research, with no particular interest in knowledge application, and being organized in the context of academic disciplines. Here, the established peers of the academic disciplines define and decide on quality (acceptance and rejection of work). Mode 2 already expresses a greater interest in knowledge application and is characterized by the following principles: "knowledge produced in the context of application," "transdisciplinarity," "heterogeneity and organizational diversity," "social accountability and reflexivity," and finally "quality control" (Gibbons et al. 1994, pp. 3–8, 167; see furthermore Nowotny et al. 2001, 2003 and 2006). "Mode 3" universities or higher education institutions (Carayannis and Campbell 2006) are inclined to seek and to explore creative, novel, and innovative combinations of Mode 1 and Mode 2. One key interest of Mode 3 is "basic research in the context of application" (Campbell and Carayannis 2013, p. 34). Mode 2 and Mode

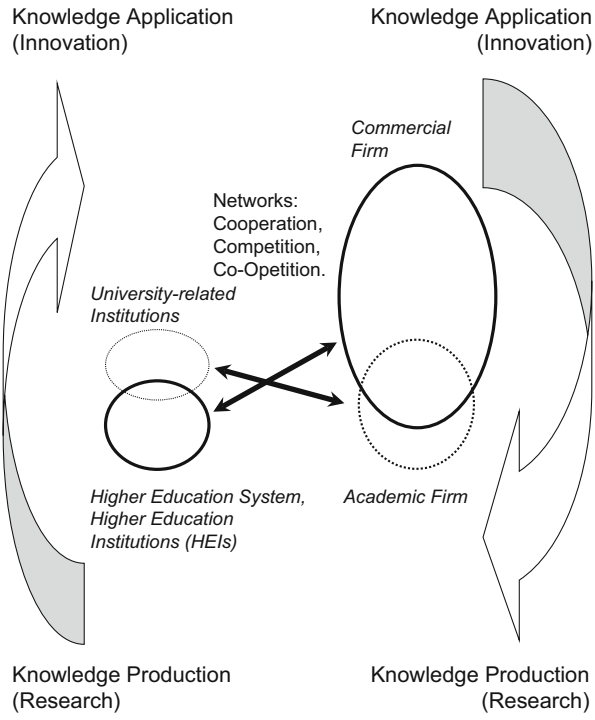


Fig. 1 Knowledge production and linear and nonlinear innovation interaction between academic firms, commercial firms, and universities (higher education institutions) (Source: Authors' own conceptualization based on Carayannis and Campbell (2009, p. 211; 2012, p. 25) and on Campbell and Carayannis (2013, p. 29))

3 universities clearly meet and fulfill some of the characteristics of the "entrepreneurial university." However, it is important to realize that a Mode 3 university is more than an entrepreneurial university, in the sense that Mode 3 universities are still interested in focusing on and in conducting basic research. But the Mode 3 university does not assume an intrinsic contradiction between basic research and innovation (knowledge application): in fact, quite contrarily the Mode 3 university sees benefits and opportunities in a parallel (nonlinear) approach to knowledge production and knowledge application, to forms of combinations between basic research and innovation. Mode 3 universities (higher education institutions) have the opportunity of offering and developing "Creative Knowledge Environments" (on creative knowledge environments, see Hemlin et al. 2004).

Mode 2 and Mode 3 higher education institutions are the perfect organizational vis-à-vis of academic firms to engage in trans-sectoral networks and to perform good knowledge production. Here, a creative and innovative hybrid overlapping in regular frequency occurs or should possibly occur. This represents a coming together and networking on equal and fair grounds. Not the universities (higher education institutions) should adapt one-sidedly to firms and their economic needs, but both sides should learn mutually from each other to the benefit of all involved parties, actors, and institutions. The assertion is "While the entrepreneurial (Mode 2) university represents a partial extension of business elements to the world of academia, the academic firm could serve as an example for an extension of the world of academia

to the world of business. Academic firms are knowledge-oriented, interested in engaging in networks with universities (the higher education sector), encourage 'academic culture and values' to motivate their employees, allow forms of academic work (such as academic-style publishing), and support continuing education and life-long learning of and for their employees (flexible time schemes, honoring life-long learning and continued continuing education with internal career promotion)" (Carayannis and Campbell 2012, p. 27).

In organizational terms, there are several possibilities, options, and opportunities, how the academic firm can be realized and can be structured (Carayannis and Campbell 2012, p. 27):

1. "A whole firm"
2. "A subunit, subdivision, or branch of a 'commercial' firm"
3. "Certain characteristics or elements of a whole (commercial) firm"

A whole firm can be organized and designed in accordance with principles of an academic firm. However, it is also possible only to organize subunits (branches) of a firm according to principles of academic firms. Alternatively, the focus may be placed primarily on certain principles of an academic firm, and these principles then can be applied to or across the whole (commercial) firm or at least to substantial divisions of the whole (commercial) firm. The term "academic firm" perhaps invites us to the belief, imagination, or vision that this would always mean a whole firm. What the analysis presented here however demonstrates is that this would be an artificially narrowing down of the concept and idea of the academic firm. It is important to note that the academic firm can address a whole firm or only specific organizational units (subunits), processes, or principles of a whole firm. In fact, this even would allow for hybrid combinations and overlapping arrangements between the academic firm (knowledge-focused and knowledge-driven) and the commercial firm (profit-driven). Currently it is difficult to assess how common or uncommon academic firms or principles of the academic firm are in the world of contemporary business. The conventional wisdom would be that the commercial firm represents (still represents) the dominant type of organizational representation for how to structure and how to develop firms (companies). In metaphorical terms, this is also the visualized image and picture in Fig. 1. With the advancement of economy and knowledge economy in the context of the knowledge society (and knowledge democracy), it is plausible to assume that expectations are justified that a diffusion and spreading of academic firms appear to be reasonable. Academic firms have all the potential of substantially transforming (in a bottom-up mode and fashion) how the economy and economic activity are being understood and processed. The academic firm invites the introduction of academic values, lifestyles, and working methods into business, because the academic firm believes that academic research and the academic context to academic research are beneficial to the capacities and capabilities of firms focusing on knowledge production (research) and knowledge application (innovation). For the academic firm, academic research is not external but is being conceptualized, remodeled, and incorporated as an intrinsic process and

an intrinsic form of organization within the boundaries of a firm. Academic firms also engage in academic research, where research is linked and interconnected with innovation. Academic firms express and encourage a "limited 'scientification' of business R&D" (Campbell and Güttel 2005, p. 170; Campbell et al. 2013; see also Carayannis and Campbell 2009).

Cross-Employment

Cross-employment represents a type of multi-employment, where a person is being employed simultaneously by more than one organization (institution). The emphasis here is placed on employment by at least two organizations, and it must be a simultaneous (and not a sequential first-then) form of employment. The opposite concept to cross-employment would be the single employment by only one organization (or institution) at a time. Employment implies that the person is involved in social and tacit learning of the different organizations that also behave as organizational environments. When employment is in reference to knowledge production and knowledge application, then cross-employment should also be understood as an expression of and as a form for organizing, optimizing, and excelling research and innovation. Cross-employment already exists as an empirical phenomenon. How common or uncommon currently cross-employment is is difficult to assess. This topic has not been sufficiently researched, so far. Beyond the empirical aspects of cross-employment, also the question could be raised, whether cross-employment has also the qualities of a normative and ideal-typical category: Should work, also in association with knowledge production, research, and innovation, be organized in a way of allowing for more (or even encouraging) arrangements that follow the logic of cross-employment?

Cross-employment as a specific term and concept was first introduced by Campbell (2011). In Carayannis and Campbell (2012, p. 24), the following comprehensive description for cross-employment is being presented: "*Cross-employment* (multi-employment) may be regarded as one (organizational) strategy for realizing creative knowledge environments. Cross-employment (multi-employment) refers to a knowledge worker, employee, who is being simultaneously employed by more than one organization, possibly being located in different sectors (e.g., a higher education and a non-higher education institution, e.g., a university and a firm). *This supports the direct network-style coupling of very different organizations in knowledge production and innovation application*, expressing, therefore, what nonlinear innovation could mean in practical terms . . . Cross-employment makes possible 'parallel careers' for individuals (knowledge workers) across a diversity of organizations and sectors, thus also a simultaneous operating in parallel in organizations with different rationales and innovation cultures." The Creative Knowledge Environments (CKEs), as a concept and term, were introduced by Hemlin et al. (2004).

Cross-employment (employment) has a hybrid overlapping or can be combined with other forms of activities that are non-employment based

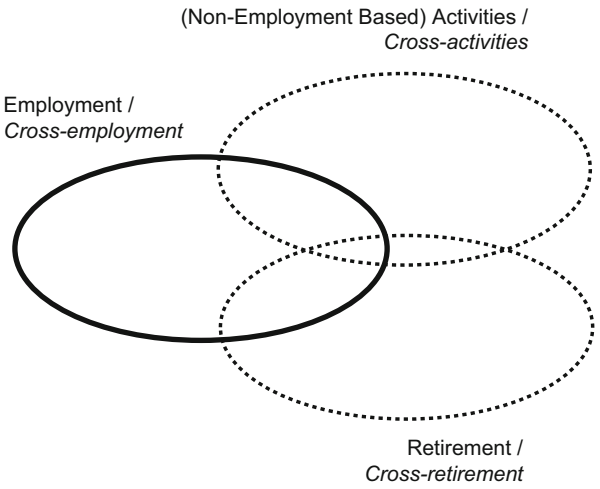


Fig. 2 The hybrid overlapping of employment and cross-employment with activities and retirement (Source: Authors' own conceptualization based on Campbell (2013))

(such as self-employment) or also with partial (part-time) retirement, then being called cross-retirement in connection with employment or cross-employment (Fig. 2). Ramifications of cross-employment, therefore, are not only limited to types of employment.

Cross-employment does not only have advantages, when compared with single employment. However, in the following those characteristics of cross-employment should be elaborated in more detail, which offer opportunities and potentially also benefits to (individual) persons as well as the organization. The context for cross-employment to be discussed here are organizations (institutions) that are engaged in knowledge production and knowledge application or research and innovation:

1. *Creative development of complementary competences, diversification, and pluralization of the competence base of organizations:* Persons that can base their activities of knowledge production and knowledge application on working relations of cross-employment are in a position of creatively (and innovatively) developing further complementary competences that also refer to practical experiences and tacit knowledge. For the organization, this has the potential benefit that the spectrum of competences of their employees is being diversified and pluralized to a crucial extent. This supplies evidence how cross-employment represents one approach for helping to develop "creative knowledge environments" within organizations. The combination of complementary competences also nurtures the creation of new competences. Organizations (institutions), therefore, should regard cross-employment also as an organizational opportunity for themselves.
2. *Network-style formation of linkages (and bridges) across organizations and sectors:* Cross-employment supports the formation and advancement of networks and network linkages between organizations (institutions). In fact, cross-employment represents a crucial form of organizational manifestation for the

development and promotion of networks. For example, there can be cross-employment between two or more universities (higher education institutions), where in one case the employee may focus on academic research and in the other case on organizational quality enhancement. In such a scenario, the cross-employment would unfold still within one sector, the higher education system. Cross-employment, however, can also create network-style connections between organizations in different sectors, for example, the higher education sector and the economy (the business enterprise sector): in such a scenario, the cross-employment would act and behave trans-sectorally and would perform a trans-sectoral building of linkages and bridges. Multiple forms, networks, and combinations of trans-sectoral cross-employment between universities (higher education institutions), university-related institutions, firms (commercial firms, academic firms), and other organizations (e.g., of the civil society) are possible, feasible, and even recommendable (see Fig. 2). Cross-employed persons, across different organization and sectors, create (or at least have the potential of creating) a multitude or heterogeneity of cross-organizational and cross-sectoral networks.

3. *Cross-employment as one organizational expression for nonlinear innovation:* The model of linear innovation is often being referred to Vannevar Bush (1945). One core understanding of that model is that first there is basic research in a university context, which later develops further to an innovation application in the context of a firm. This linear framing of innovation is being challenged by the notions of an evolving nonlinear innovation. In practice, there often will be a hybrid overlapping of forms and processes of linear and nonlinear innovation. This may mean that an organization (firm) engages simultaneously in different technology life cycles at different degrees (levels) of technology maturity (closer to basic research or closer to application and market commercialization). Cross-employment represents another crucial manifestation and organizational representation of and for nonlinear innovation. For example, a cross-employed person (knowledge worker) can participate in basic research at a university and, at the same time, may be involved in innovation application and knowledge practice in a firm or another organization outside of university. Such a person works simultaneously at both ends of the whole spectrum of knowledge production and knowledge application.

The concept "cross-retirement" here means (see again Fig. 2): "Cross retirement (i.e., cross-employed and cross-retired) likewise aims at allowing the individual to combine the benefits of retirement and those of work in a similar way, but with some important distinctions. Cross-retirement (a) does not constitute a transition period but rather an additional phase of life without any pre-determined endpoint, and (b) the ratio of work and free time should be self-determined and flexibly adjustable to the individual's needs. Cross-retirement thus should enable the individual to continue to contribute to society while limiting the restraints of regular employment. Cross-retirement represents a status where a person is retired and works at the same time. More precisely defined, this means that a person works (full-time, but probably more likely part-time), however also earns retirement payments, to which he or she is eligible and entitled" (Blasche and Campbell 2013, p. 508).

Results and Discussion

Design (and redesign) characteristics (attributes) of the academic firm are:

1. It is knowledge-based, knowledge-creating, and innovation-oriented.
2. Incorporates academic values, motivates employees, and creates bonds of trust.
3. Engages in networks with universities (higher education institutions, HEIs) and can access university knowledge (e.g., basic university research).
4. Allows academic research work (academic publications can act as incentives for codifying tacit knowledge).
5. Supports and enables continued education, lifelong learning, and partial absence/leave of employees.
6. Allows cross-employment (split employment) of employees with other (academic) organizations and institutions.
7. It should foster "Creative Knowledge Environments" (CKE; see Hemlin et al. 2004).

Conclusion

In search for an ideal-typical portraying of the academic firm and the concept of the academic firm, the following characteristics and principles can be listed and again summarized (designed and redesigned):

1. The academic firm is a type of firm (firm-based organization or institution) that is being driven by focusing on encouraging, supporting, and advancing knowledge production (research, research and experimental development, R&D) and knowledge application (innovation). The academic firm is also interested in generating profits (revenues), but this should be a "sustainable profit" in comprehensive terms and well in balance with the good principles of a good knowledge production and knowledge application (innovation). The academic firm operates in a whole knowledge-based ecosystem.
2. The academic firm is knowledge-based, knowledge-oriented, knowledge-driven, knowledge-producing, and knowledge-creating. The academic firm displays (often) an inclination for applying and following the logic of nonlinear innovation, by this demonstrating flexibility. The academic firm regards basic research in the context of application as an opportunity.
3. The academic firm incorporates academic values to motivate its employees and to create bonds of trust and of a good relationship between the organization and the individual employees. The academic firm interprets and qualifies a disciplinary (interdisciplinary) variety of the background of its employees (and their competences) as a potential opportunity and asset to perform creatively in knowledge production and knowledge application.
4. The academic firm has an interest to engage in networks with universities (higher education institutions) or other academic research institutions, driven out of a

desire to access university knowledge (e.g., basic university research). In general, the academic firm values engagement in diversified networks as a form for creating knowledge as well as benefitting from opportunities.
5. The academic firm allows and encourages academic research work (academic publications can act as incentives for employees to codify their tacit knowledge).
6. The academic firm supports continuing education, further education, and lifelong learning of its employees and has in principle a positive attitude in favor of a flexibility concerning the load of working hours and their flexible adaptation for their employees and their needs (full-time, part-time, perhaps shifting back-and-forth) but also for partial absence or partial leave of its employees. Cross-benefitting cross-connections between careers and career schemes with continuing education are being explored by the academic firm.
7. The academic firm accepts in principle, in certain situations even promotes, split employment or "cross-employment" (multi-employment) of its employees with other (academic) organizations or institutions, for example, universities or other higher education institutions.
8. The academic firm is interested in creating internally "Creative Knowledge Environments" (Hemlin et al. 2004) within the internal boundaries of its organization. The academic firm emphasizes the need of and for creativity for knowledge (knowledge production, research) and innovation.

The academic firm has the potential of transforming and changing the way how knowledge-based and knowledge-oriented economic work is being organized and performed.

However, does the academic firm represent primarily an ideal-typical concept, or does the academic firm exist (do academic firms exist) also in real terms? The commercial firm appears to define the dominant and established norm in the world of contemporary business. The empirical appropriateness or the proof of fitness for the ideas of the academic firm perhaps still needs to be demonstrated or verified. Academic firms are or would be exposed to an economic environment, where success often means to cope with and to profit from mechanisms and forces of severe competition in a continuously globalizing world. But the concept of "co-opetition" (Brandenburger and Nalebuff 1997) suggests also that success in competition means to develop networks with overlapping patterns of cooperation and competition. Between the two (conceptually) extreme poles of the academic firm and the commercial firm, many and several in-between forms of organization or hybrid combinations are possible. *The academic firm represents a challenging proposition for current business. The academic firm, however, indicates also routes and paths, for how next-stage changes and future changes and future successes in the world of business and the knowledge economy (in the knowledge economy) can be approached and achieved.* The academic firm is interested in bringing together innovation and entrepreneurship for development, more so for sustainable development.

The proposition here is that the academic firm represents a new design (and redesign) for entrepreneurship in innovation-driven knowledge economy.

Cyber development can be defined as a development in terms of a sustainable development of knowledge economy, knowledge society, and knowledge democracy that is knowledge-based and knowledge-driven and where innovation is playing a crucial role. In this understanding, the academic firm has all the capabilities and capacities to contribute to this type of development and cyber development, by this adding to progress in and advancement of knowledge economy.

Cross-References

- ▶ Epistemic Governance and Epistemic Innovation Policy in Higher Education for Cyber-Development
- ▶ Quadruple and Quintuple Helix Innovation Systems and Mode 3 Knowledge Production
- ▶ Quality of Democracy in Quadruple Helix Structures: OECD Countries in Global Comparison

References

Blasche, G. W. E., & Campbell, D. F. J. (2013). Cross-retirement (Cross-employed cross-retired) and innovation. In E. G. Carayannis (Editor-in-Chief), I. N. Dubina, N. Seel, D. F. J. Campbell, D. Uzunidis (Associate Editors) (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 508–513). New York: Springer. http://link.springer.com/referenceworkentry/10.1007/978-1-4614-3858-8_255

Brandenburger, A. M., & Nalebuff, B. J. (1997). *Co-opetition*. New York: Doubleday.

Bush, V. (1945). *Science: The endless frontier*. Washington, DC: United States Government Printing Office. http://www.nsf.gov/od/lpa/nsf50/vbush1945.htm#transmittal

Campbell, D. F. J. (2011). Wissenschaftliche „Parallelkarrieren" als Chance. Wenn Wissenschaft immer öfter zur Halbtagsbeschäftigung wird, könnte eine Lösung im „Cross-Employment" liegen. Guest Commentary for DIE PRESSE (2 Feb 2011). http://diepresse.com/home/bildung/meinung/635781/Wissenschaftliche-Parallelkarrieren-als-Chance?direct=635777&_vl_backlink=/home/bildung/index.do&selChannel=500

Campbell, D. F. J. (2013). Cross-employment. In E. G. Carayannis (Editor-in-Chief), I. N. Dubina, N. Seel, D. F. J. Campbell, D. Uzunidis (Associate Editors) (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 503–508). New York: Springer. http://link.springer.com/referenceworkentry/10.1007/978-1-4614-3858-8_254

Campbell, D. F. J., & Carayannis, E. G. (2012). Lineare und nicht-lineare Knowledge Production: Innovative Herausforderungen für das Hochschulsystem. *Zeitschrift für Hochschulentwicklung, 7*(2), 64–72. http://www.zfhe.at/index.php/zfhe/article/view/448

Campbell, D. F. J., & Carayannis, E. G. (2013). *Epistemic governance in higher education. Quality enhancement of universities for development*. Springerbriefs in business. New York: Springer. http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6

Campbell, D. F. J., & Güttel, W. H. (2005). Knowledge production of firms: Research networks and the "scientification" of business R&D. *International Journal of Technology Management, 31*(1/2), 152–175.

Campbell, D. F. J., Carayannis, E. G., & Güttel, W. H. (2013). Academic firm. In E. G. Carayannis (Editor-in-Chief), I. N. Dubina, N. Seel, D. F. J. Campbell, D. Uzunidis (Associate Editors) (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 17–23). New York: Springer. http://link.springer.com/referenceworkentry/10.1007/978-1-4614-3858-8_252

Carayannis, E. G., & Campbell, D. F. J. (2006). "Mode 3": Meaning and implications from a knowledge systems perspective. In E. G. Carayannis & D. F. J. Campbell (Eds.), *Knowledge creation, diffusion and use in innovation networks and knowledge clusters* (pp. 1–25). Westport: Praeger.

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "Quadruple helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46*(3/4), 201–234. http://www.inderscience.com/browse/index.php?journalID=27&year=2009&vol=46&issue=3/4 and http://www.inderscience.com/search/index.php?action=record&rec_id=23374&prevQuery=&ps=10&m=or

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development*. Springerbriefs in business. New York: Springer. http://www.springer.com/business+%26+management/book/978-1-4614-2061-3

Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P., & Trow, M. (1994). *The new production of knowledge. The dynamics of science and research in contemporary societies*. London: Sage.

Hemlin, S., Allwood, C. M., & Martin, B. R. (2004). *Creative knowledge environments. The influences on creativity in research and innovation*. Cheltenham: Edward Elgar.

Nowotny, H., Scott, P., & Gibbons, M. (2001). *Re-thinking science. Knowledge and the public in an age of uncertainty.* Cambridge: Polity Press.

Nowotny, H., Scott, P., & Gibbons, M. (2003). Mode 2 revisited: The new production of knowledge. *Minerva, 41*, 179–194.

Nowotny, H., Scott, P., & Gibbons, M. (2006). Re-thinking science: Mode 2 in societal context. In E. G. Carayannis & D. F. J. Campbell (Eds.), *Knowledge creation, diffusion, and use in innovation networks and knowledge clusters. A comparative systems approach across the United States, Europe and Asia* (pp. 39–51). Westport: Praeger.

Epistemic Governance and Epistemic Innovation Policy in Higher Education for Cyber-Development

4

David F. J. Campbell and Elias G. Carayannis

Contents

Abstract

Epistemic governance and epistemic innovation policy formulate a critique against too-narrowly defined approaches to governance, where governance follows one-sidedly bureaucratic or technocratic considerations. Instead, epistemic governance (also quality management and quality enhancement) and epistemic innovation policy should be regarded as a plea for a more comprehensive understanding, where the explicit-making, comprehension, and reflection of

D. F. J. Campbell (✉)
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (Iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@aau.at; david.campbell@uni-ak.ac.at; david.campbell@univie.ac.at

E. G. Carayannis
Department of Information Systems and Technology Management, School of Business, The George Washington University, Washington, DC, USA
e-mail: caraye@gwu.edu

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_58

knowledge, knowledge production, and knowledge application are keys for a successful governing and governance. For the further progress of advanced knowledge society, advanced knowledge economy, and advanced knowledge democracy, universities and the higher education sectors are crucial for driving development. How should the governance of higher education, the quality enhancement of universities, and the careers of academic faculty (the academic profession) be organized? Epistemic governance introduces here a novel approach and understanding. Epistemic governance emphasizes that the underlying epistemic structure, the underlying epistemic base, or the underlying epistemic paradigms (knowledge paradigms) of those organizations, institutions, or systems (sectors), which should be governed, are being addressed. This defines a benchmark and set of criteria for internal and external governance in higher education that is interested in applying a good, effective, and sustainable governance. Quality assurance, quality enhancement, and quality management of higher education, from the perspective of epistemic governance, should also orient themselves to quality and quality dimensions that cross-refer to the underlying epistemic structure of higher education. In a traditional understanding, the academic career patterns of the academic core faculty at universities follow a tenure track logic. Cross-employment (multi-employment), on the contrary, refers to academic faculty (the academic profession) with simultaneous employment contracts to more than one organization only within or both inside and outside of higher education. Epistemic governance, in combination with cross-employment, should add to the organizational flexibility and creativity of universities and other higher education institutions, supporting the integration of a pluralism and diversity of knowledge production (basic research in the context of knowledge application and innovation), the formation of nonlinear innovation networks, and providing a rationale for a new type of academic career model.

Keywords

Cross-employment · Cyber development · Epistemic governance · Epistemic innovation policy · Higher education · Innovation · Knowledge paradigms · Linear innovation · Mode 1 and Mode 2 knowledge production system · Mode 3 knowledge production system · Nonlinear innovation · Quadruple Helix innovation systems · Quality · Quality enhancement · Quintuple Helix innovation systems

Introduction

The concept of epistemic governance is based on the understanding that the underlying epistemic structure, the underlying epistemic base, and the underlying epistemic paradigms of those organizations, institutions, or systems (sectors) are being addressed, which should be governed. In the context of higher education, governance can refer to internal governance within a university (higher education institution) or within the higher education system but also to external governance, for

example, governance measures of a government for universities. A more detailed definition of epistemic governance would stress: "'Epistemic' governance of and in higher education therefore requires that the underlying epistemic structure of higher education and, more particularly, also the underlying paradigms of the produced knowledge are being addressed. Epistemic governance refers directly to the underlying 'knowledge paradigms' of higher education that carry and drive higher education" (Campbell and Carayannis 2013a, p. 27). Here, in this definition, the focus is placed on "epistemic" in the context of "epistemic governance." Consequently, one important implication therefore is "good, sustainable and effective (external and/or internal) governance of organizations, institutions or systems (sectors) is in the long run only possible, when the underlying epistemic structure, the underlying epistemic base or the underlying epistemic paradigms" are indicated (Campbell and Carayannis 2013a, p. 27). The epistemic structure reveals, also, what the self-rationale of an organization or a system is. Alternative definitions of epistemic governance may lean more toward the aspect of governance within the context of epistemic governance: "In this context the conceptual framework of 'epistemic governance' aims to address the power relations in the modes of creating, structuring, and coordinating knowledge on socio-ecological issues. . . . Finally, the production and use of knowledge is seen to be linked to questions of relational, structural, and soft power, and to the relationship between science and policy" (Vadrot 2011, p. 50). Vadrot (2011) introduced the concept of epistemic governance to academic debate in reference to social ecology. Campbell and Carayannis (2013a) were the first to apply the concept of epistemic governance to higher education.

The Conceptual Definition of Epistemic Governance and of Epistemic Innovation Policy

Is it possible that there is an organization, institution, or system without an underlying epistemic structure? This may (or may not) be true for some organizations or institutions; however, for a whole system or sector, this appears to be unlikely and improbable. Particularly in the case of universities, higher education institutions, and higher education systems, it is evident that these rely, operate, and behave on the basis of an underlying epistemic structure. "Knowledge paradigms" refer to the conceptual understanding of knowledge production (research) and knowledge application (innovation) in the higher education system (universities) or the economy (firms). For describing and explaining how knowledge production is functioning within the higher education sector or a university-type system, the concepts of "Mode 1" and "Mode 2" of knowledge production were introduced more recently (Gibbons et al. 1994; see also Nowotny et al. 2001, 2003, 2006). University research in a traditional understanding of Mode 1 concentrates on basic research, mostly organized within the matrix of academic disciplines, and not formulating a particular interest for the practical use of knowledge and innovation. Mode 1 is being challenged by Mode 2. Mode 2 expresses a greater interest for knowledge application and a knowledge-based problem-solving by referring to the following principles:

"knowledge produced in the context of application," "transdisciplinarity," "heterogeneity and organizational diversity," "social accountability and reflexivity," and "quality control" (Gibbons et al. 1994, pp. 3–8, 167). Success and quality are being approached and defined differently in the analytical architecture of Mode 1 and the Mode 2. For Mode 1, the answer is: "academic excellence, which is a comprehensive explanation of the world (and of society) on the basis of 'basic principles' or 'first principles', as is being judged by knowledge producer communities (academic communities structured according to a disciplinary framed peer review system)." For Mode 2, success and quality are a "problem-solving, which is a useful (efficient, effective) problem-solving for the world (and for society), as is being judged by knowledge producer and knowledge user communities" (Campbell and Carayannis 2013a, p. 32). Mode 3 knowledge production represents the conceptual and organizational attempt of trying to combine Mode 1 with Mode 2 (Carayannis and Campbell 2006, 2009, 2012). A Mode 3 university, higher education institution, or higher education system is a type of organization or system that explores ways and approaches of integrating different principles of knowledge production and knowledge application (such as Mode 1 and Mode 2), thus promoting diversity and heterogeneity but also creating creative and innovative organizational contexts for research, teaching (education), and innovation. Therefore, Mode 1, Mode 2, and Mode 3 qualify as examples for "knowledge paradigms" in higher education.

Quality management (QM) within universities or other higher education institutions refers to quality assurance but increasingly also to quality enhancement. Advances in the quality of a university and support of university development represent objectives of quality management. Therefore, also quality management should be designed, implemented, processed, and developed in accordance with the principles of epistemic governance: "This emphasizes our understanding that all forms of comprehensive and sustainable quality management in higher education must also refer to the underlying epistemic structure of higher education (at least implicitly)" (Campbell and Carayannis 2013a, p. 27). For example, it makes a difference whether a university or university unit operates according to Mode 1 or Mode 2 or a combination of both in Mode 3. This must be reflected by the specifically applied approaches in governance and quality management. For that purpose, it appears also to be necessary to connect and to link the underlying epistemic structure and the knowledge paradigms to concrete "quality dimensions," so that governance and quality management can refer to knowledge paradigms as well as quality dimensions. Possible quality dimensions are quality, efficiency, relevance, viability (sustainability), and effectiveness (Campbell 2003, p. 111; Campbell and Carayannis 2013a, p. 52). When knowledge paradigms are being translated into quality dimensions, this may make it then for governance and quality management easier to address epistemic issues in relation to knowledge production but also knowledge application. According to Ferlie et al. (2008, 2009), there exist currently two main narratives of and for governance in higher education: New Public Management (NPM) governance and network governance. While NPM already appears to be more conventionally established, network governance represents a more radical frontier for contemporary governance, with not so clear implications, fostering perhaps a demand for creating also new types of

organizational manifestation in higher education. "Cross-employment" (Campbell 2011; Campbell and Carayannis 2013a) may serve here as one possible example, where one and the same person is being simultaneously employed by more than one organization (by at least two organizations), either within higher education or trans-sectorally connecting higher education with organizations outside of higher education. Cross-employment qualifies as a form of multi-employment.

Ramifications of epistemic governance should also be thought about in a wider context. Principles of epistemic governance apply to innovation and innovation policy as well and the concept of "epistemic innovation policy." Innovation policy should address the underlying epistemic structure and knowledge paradigms of the innovation and type of innovation to be governed. Two examples for knowledge paradigms in context of innovation are linear innovation and nonlinear innovation. The more traditional model of linear innovation is being frequently referred to the concepts of Vannevar Bush (1945). The core understanding here is: the linear model of innovation underscores that first there is basic research in a university context. Gradually and step-by-step, this university research diffuses out into society and the economy. Firms and the economy as a whole pick up these lines of university research and develop them further into knowledge application and innovation, with the goal and interest of creating economic and commercial success and success stories in markets outside of higher education. Within the model of linear innovation, there operates a sequential first-then relationship between basic research (knowledge production) and innovation (knowledge application). Nonlinear innovation follows a different logic (Campbell and Carayannis 2012). The model of nonlinear innovation expresses an interest in drawing more direct connections between knowledge production and knowledge application. Here, basic research and innovation are being coupled together not in a first-then but within the structural design of an "as well as" and "parallel" (parallelized) relationship (Campbell and Carayannis 2012). Networks for nonlinear innovation operate differently than networks of linear innovation but may overlap substantially. Examples for nonlinear innovation are either firms or other types of organizations operating across a variety or ensemble of technology life cycles with differing degrees of technology maturity on the one hand or specific constellations of cross-employment on the other hand, where persons work (at the same time) concurrently at organizations, where in one case the organization (organizational unit) focuses on knowledge production but in the other case on knowledge application. Nonlinear innovation also cross-connects to Mode 3 knowledge production. One key interest of Mode 3 is to encourage and to promote "basic research in the context of application" (Campbell and Carayannis 2013a, p. 34). Furthermore, also Mode 2 appears to be compatible with a more nonlinear logic of innovation (see Fig. 1).

Results and Discussion

In the following, we want to review some of the dominant paradigms of knowledge and knowledge production in the higher education sector that currently exist or coexist (see Fig. 2 for a conceptual summary in visualization):

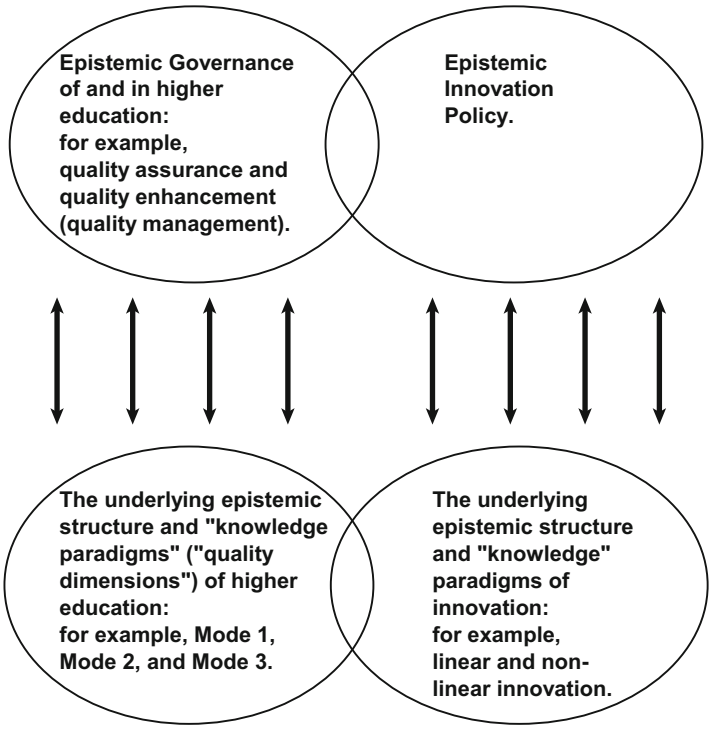


Fig. 1 Epistemic governance of and in higher education and epistemic innovation policy (Source: Authors' own conceptualization based on Campbell and Caraynnis (2013a, p. 28, b))

1. *Linear and nonlinear models of innovation, the Triple Helix, Quadruple Helix and Quintuple Helix model of innovation and the Creative Knowledge Environments*: The linear model of innovation is being conventionally ascribed to Vannevar Bush, as, for example, is being asserted by Narin et al. (1997, p. 318), even though Bush himself, in his famous report *Science: The Endless Frontier*, even never mentioned the word "innovation" (Bush 1945): this observation can be verified easily by a word retrieval command of the indicated (electronic) document. In a modern policy context, it probably would be unthinkable that such a comprehensive and important macro-level strategy paper has no explicit references to innovation. We see here to which extent the word and term of "innovation" already has diffused out into our everyday professional language during the course of the last half century. But this certainly was not the case before or earlier in the twentieth century. It could be argued, however, that Bush (1945) referred to innovation implicitly. What does the concept of linear innovation mean and imply? Referring to research, the implications are universities and the higher education sector, in general, focus on basic research that is mostly publicly financed. Gradually, from the higher education sector outward and in some "laissez-faire" fashion, university basic research diffuses out into society and

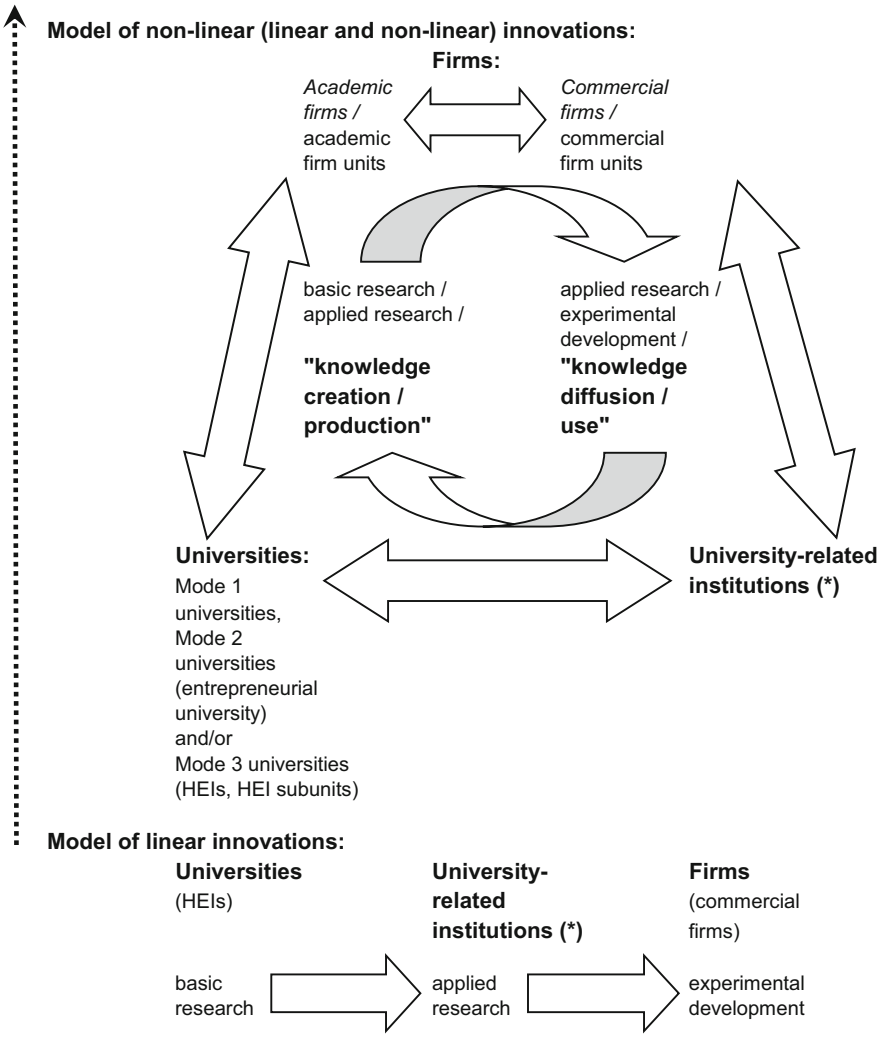


Fig. 2 The evolution of linear innovation systems only to a combination of linear and nonlinear innovation systems (Source: Authors' own conceptualization based on Carayannis and Campbell (2009, p. 211, 2012, p. 25). (*) University-related may be translated into the German languages as "außeruniversitär" (Campbell 2003, p. 99))

the economy. Finally, the economy and different business firms pick up some of these basic research lines and convert them into applied research and experimental development, out of an interest to create commercial products and services that can be marketed and sold with profit. Applied research and even more so experimental development, therefore, are being carried out in the business

enterprise sector and are being mostly privately financed (in less mature industries and less advanced economies, the public financing may be more important). There operates a *first-then sequential order* from basic research to applied research and then to experimental development. Nonlinear models of innovation, on the contrary, are also inclined to focus on *"parallel" effects or the simultaneous engagement of universities and firms* in basic research as well as applied research and experimental development: "In contrast to the linear model, the paralleling of basic research, applied research and experimental development demands that the different R&D activities should be considered, to phrase it in a challenging language, as 'parallel processes'" (Campbell and Güttel 2005, p. 167; see also Campbell 2000). At the organizational or institutional microlevel (meso-level), distinct linear-innovation-lines still may operate. However, at the meso-level or macro-level, the organization or institution has opportunities of participating in different linear-innovation-lines at different stages. *What results is that universities and firms carry out and perform basic research, applied research, and experimental development at the same time; R&D is being and becoming paralleled. The sequential first-then relationship is transformed into a "first-first" relationship*. One key challenge focuses now on setting up research designs, where there is a cross-learning and cross-fertilization between different linear-innovation-lines or research lines. *We may experience here an overlapping of liner and non-liner innovation, generating, all together, a system of nonlinear innovation* (compare also with Carayannis and Campbell 2012, p. 25). When universities engage in applied research and firms in basic research, this creates opportunities (but also needs) for more hybrid and network-based linkages between universities and firms but perhaps also between universities and other organizations: university-related institutions but also the "media-based and culture-based public" and "civil society" in Quadruple Helix innovation arrangements (Carayannis and Campbell 2009, p. 207; 2011, pp. 13–14; 2012, pp. 13–14; see also: Danilda et al. 2009). The Quintuple Helix, ultimately, integrates the "environment or the natural environments" into the overall architecture of innovation systems (Carayannis and Campbell 2010, pp. 61–62). "The Quintuple Helix finally embeds the Quadruple Helix (and the Triple Helix) in context of the environment or the natural environments" (Carayannis and Campbell 2010, pp. 61–62). Furthermore: "The Quintuple Helix model is interdisciplinary and transdisciplinary at the same time: the complexity of the five-helix structure implies that a full analytical understanding of all helices requires the continuous involvement of the whole disciplinary spectrum, ranging from the natural sciences (because of the natural environment) to the social sciences and humanities (because of society, democracy and the economy). The Quintuple Helix also is transdisciplinary, since it can be used as a frame of reference for decision-making in connection to knowledge, innovation and the (natural) environment" (Carayannis and Campbell 2011, p. 62; see also Campbell and Campbell 2011, pp. 15–16, 23–27). The university-industry-government relations of the Triple Helix model of knowledge production and innovation address such interactions and interferences, by speaking in this context of "trilateral networks

and hybrid organizations" (Etzkowitz and Leydesdorff 2000, p. 111). Universities increasingly could (should) learn business management skills and competences, but also firms could (should) open themselves for the academic world. This creates niches and opportunities for the "entrepreneurial university" (Etzkowitz 2003) and the "academic firm" (Campbell and Güttel 2005, pp. 170–172). Academic firms and commercial firms may coexist and coevolve. While the concept of the commercial firm focuses on profit and profit maximization, *the concept of the academic firm is interested in developing social environments that foster academic (academic style) knowledge creation and creative knowledge production* that are not dissimilar to university contexts, for example, also engaging some of their knowledge work efforts in publishing activities and academic publications (Carayannis and Campbell 2009, pp. 211–212). An academic firm may be a whole firm or a subunit, subdivision, or branch of a "commercial" firm or represent certain "characteristics" of a whole (commercial) firm such as supporting continuing education, lifelong learning, and partial absence (leave, sabbaticals) of employees or allowing split "cross-employment" (Campbell 2011) of their employees with other organizations, most notably academic institutions (higher education institutions) (Carayannis and Campbell 2012, pp. 24–28). Universities (entrepreneurial universities) and firms (academic firms), of course, cannot and should not coincide completely; there still must operate some distinct differences. These manifold mutual hybrid overlappings and networks of knowledge and innovation, in which universities, entrepreneurial universities, and commercial and academic firms interplay should also foster developing and creating "Creative Knowledge Environments" that are defined as (Hemlin et al. 2004, p. 1): "Creative knowledge environments (CKEs) are those environments, contexts and surroundings the characteristics of which are such that they exert a positive influence on human beings engaged in creative work aiming to produce new knowledge or innovations, whether they work individually or in teams, within a single organization or in collaboration with others."

2. *Mode 1 and Mode 2 of knowledge production:* Gibbons et al. (Gibbons et al. 1994) focus on analyzing key principles of knowledge, of knowledge that roots in knowledge production in higher education (universities) and then diffuses out into society and the economy. One may formulate the proposition that the term "knowledge production" in Gibbons et al. (1994) already incorporates the whole spectrum of "knowledge production" and "knowledge creation." An attempted distinction could emphasize that in context of higher education, knowledge creation is more basic or fundamental than knowledge production. However, throughout the whole text here, the terms of knowledge creation and knowledge production are being used in an interchangeable way and manner. Their conceptual starting point is the "Mode 1" production of knowledge, referring to (mid-term or long-term) basic university research that expresses no major interests in innovation and knowledge application and which is structured and organized according to a disciplinary logic (see Gibbons et al. 1994, pp. 1, 3, 8, 24, 33–34, 43–44, 167). Mode 1 is being challenged by the new "Mode 2" of knowledge production that is being driven by the following principles: (1) "knowledge

produced in the context of application," (2) "transdisciplinarity," (3) "heterogeneity and organizational diversity," (4) "social accountability and reflexivity," and (5) "quality control" (Gibbons et al. 1994, 3–8, 167). Mode 2 grew out of Mode 1, and Mode 2 coevolves with Mode 1 (Gibbons et al. 1994, pp. 14, 17). Mode 1 coincides with a traditional understanding or picture of universities and of university research, whereas Mode 2 focuses more on the integration of knowledge production of the universities into and with the knowledge production of society and of the economy. Mode 2 university research is directed toward problem-solving, thus emphasizing the applicability and usability of university-created knowledge for the needs of society and of the economy. Implications of Mode 2 are that the whole spectrum of basic research, applied research, and experimental development is being reframed into a context of application. This emphasis on application, however, certainly does not imply that basic research becomes replaced by applied research. This would be a misperception or wrong interpretation (Gibbons et al. 1994, pp. 4, 33–34). There occur to be an increasing overlapping of "discovery," on the one hand, and the "application" and "fabrication" of knowledge on the other (also experimentation and simulation). By applying knowledge, also new knowledge is being discovered. Epistemic implications may be that (at least partially) knowledge application is necessary for further enhancing basic research, in the sense of some overlapping of linear and nonlinear innovation modes. Application feeds back, also into basic research, thus supporting the further development and creation of theories. Application is also important for "continuous innovation" (on Mode 1 and Mode 2, see furthermore Nowotny et al. 2001, 2003, 2006; Scott 2009; Campbell 2006, pp. 71–73, 91–92; Carayannis and Campbell 2010, pp. 48–52). For Mode 1 knowledge as well as Mode 2 knowledge, the quality, of course, is key. However, quality is being differently defined in these two domains. Quality according to "Mode 1" is *academic excellence, which is a comprehensive explanation of the world (and of society) on the basis of "basic principles" or "first principles," as is being judged by knowledge producer communities (academic communities structured according to a disciplinary framed peer review system).* Quality according to "Mode 2" is *problem-solving, which is a useful (efficient, effective) problem-solving for the world (and for society), as is being judged by knowledge producer and knowledge user communities.* Mode 1 and Mode 2 certainly qualify to be interpreted as "knowledge paradigms" that underlie higher education (on paradigms, see also Kuhn 1962).

3. *Mode 3 knowledge and Mode 3 universities (higher education systems):* Mode 3, as a concept (and as a metaphor), emphasizes that there can exist and coexist very different types of knowledge and also very different paradigms of knowledge. Innovation represents applied knowledge. Mode 3 stresses also the importance of this coexistence and coevolution of different knowledge and innovation modes and paradigms. "'Mode 3' allows and emphasizes the co-existence and co-evolution of different knowledge and innovation paradigms. In fact, a key hypothesis is: *The competitiveness and superiority of a knowledge system is highly determined by its adaptive capacity to combine and integrate different*

knowledge and innovation modes via *co-evolution, co-specialization and co-opetition knowledge stock and flow dynamics* (for example, Mode 1, Mode 2, Triple Helix, linear and non-linear innovation)" (Carayannis and Campbell 2009, p. 223). This pluralistic structure and design of Mode 3 indicates potentials of congruence between Mode 3 and democracy. "Pluralism of knowledge modes" and "Democracy of Knowledge" interrelate (Carayannis and Campbell 2009, pp. 208, 224). This makes plausible why also advanced Mode 3 knowledge and knowledge-based democracies and knowledge democracies interrelate. Therefore, one can assert and claim a coevolution of knowledge societies, knowledge economies, and knowledge democracies (Carayannis and Campbell 2010, pp. 52–58). "Mode 3 claims a certain congruence of structures and processes of advanced knowledge and advanced democracy" (Carayannis and Campbell 2010, p. 52). *As a Mode 3 higher education system (higher education sector) qualifies a higher education system that operates simultaneously according to different paradigms (and types) of knowledge and innovation. A Mode 3 higher education system perceives and assesses such a pluralism, coexistence, and coevolution of different paradigms (and types) of knowledge and of innovation also as positive and as necessary for advancing higher education, the society and economy (and democracy) in the "age of knowledge."* Epistemic governance, externally and internally, is directed toward the different knowledge paradigms that underlie higher education. One implication is that in Mode 3 higher education, the Mode 1 and Mode 2 (Mode 1 and Mode 2 knowledge production) coexist and may be coupled in creative organizational designs, perhaps based on networks or network-style arrangements. Such a coupling of and in Mode 1 and Mode 2 may also create a sustainable surplus and other synergies in knowledge creation and knowledge production of the higher education sector, so necessary for knowledge societies and knowledge economies, also featuring the "creativity economy" (Dubina et al. 2012). One may even set up the proposition for discussion that de facto all higher education systems in advanced societies are Mode 3. However, an "advanced Mode 3 higher education system" would make this also explicit, emphasizing that this pluralism, coexistence, and coevolution of knowledge paradigms are being acknowledged and are being valued positively. A Mode 3 higher education system enables and favors very different combinations of different types and paradigms of knowledge and knowledge production. *Higher education institutions can be organized according to Mode 1, Mode 2 (the "entrepreneurial university"), or Mode 3, then implying that higher education institutions are interested in covering Mode 1 and Mode 2, allowing both to exist explicitly but also setting up creative Mode 3 designs of a cross-referencing that should create a surplus in high-quality knowledge production*. For example, Mode 1, Mode 2, and Mode 3 can exist at the level of the whole university or at specific sublevels, such as faculties (schools) or university departments. From an organizational developmental perspective, a whole spectrum of various strategies, options, or profiles opens up for universities and the university subunits. Nothing should be precluded; *in fact we could imagine a coexistence and coevolution of Mode 1 universities, Mode 2 universities*

(entrepreneurial universities), and Mode 3 universities and of Mode 1, Mode 2, and Mode 3 university subunits. This hybrid and creative overlapping of Mode 1 (linear innovation), Mode 2 (entrepreneurial university), and Mode 3 (nonlinear innovation) universities and university subunits additionally offers opportunities for implementing and promoting "Creative Knowledge Environments" (Hemlin et al. 2004). Creativity is essential for producing new knowledge in higher education: "That line of thinking emphasizes to interpret new knowledge as a creative knowledge. Or to rephrase: new knowledge qualifies as a potential candidate for a creative knowledge. . . .*Without creativity, the knowledge input for the innovation process might face serious constraints*" (Carayannis and Campbell 2010, pp. 47–48). In several contexts, networks can offer representing the dominant organizational approach of linking together and combining Mode 1, Mode 2, and Mode 3 knowledge production. *At the aggregated level of the whole national innovation system, a hybrid dynamics of a knowledge coevolution of Mode 1, Mode 2, and Mode 3 universities and university subunits, on the one hand, and of commercial and academic firms and firm subunits, on the other, may unfold and drive further the next-step advancements of knowledge societies, knowledge economies, and knowledge democracies. This may also refer to other levels (subnational, supranational, transnational) of the architecture of multilevel innovation systems* (Carayannis and Campbell 2012, pp. 32–35). To a certain extent, this "Mode 3 university" can be understood as the epistemic concept as well as the organizational developmental concept, how to make possible and to foster a combination and coevolution of Mode 1 and Mode 2 knowledge production in university context. If true, this coevolution would generate and create a crucial knowledge production surplus. Mode 1 knowledge production distinguishes between basic research and applied research. The Mode 3 emphasis (*shift of emphasis*) in knowledge production may be to focus, instead, more on "basic research in the context of application." Mode 3 also encourages interdisciplinarity and transdisciplinarity (on a further discussion of interdisciplinarity or "Interdisziplinarität," see also Markus Arnold 2009, pp. 65–97). In a shortcut, *transdisciplinarity may be defined as the application of interdisciplinarity* (transdisciplinarity = application of interdisciplinarity?). The Mode 3 inclination for a basic research in context of application highlights a possible route of further development for transdisciplinarity (and interdisciplinarity). For interesting, creative, and innovative examples of integrating and analytically combining research in fields and disciplines of the social sciences and natural sciences, see also furthermore Gottweis (1998), Hindmarsh and Prainsack (2010), and Prainsack and Wolinsky (2010).

4. *Academic faculty (academic profession), academic "cross-employment," and academic "cross-careers" inside and outside of higher education:* In the world of Mode 1 universities or Mode 1 university subunits, at least in conceptual terms, the status and the career schemes of the academic faculty (or of the academic profession) at higher education institutions appear to be clearer and more evident. There is a "core faculty," interested in achieving tenure and dominating the top hierarchy positions at the university. Anyone who is not core faculty and wants to

stay within the university tries to become a member of the core faculty. Knowledge production (university research, basic university research) of Mode 1 is directed toward "academic excellence," as is being verified (or falsified) by peers in peer review against the background and logic of the academic disciplines. Academic excellence, in Mode 1, coincides to a large extent with assessment results of a disciplinary-based peer review. The linear-innovation-tendency of Mode 1 also implies that either you work within the university or you work outside of the university, then for a firm or a different organization in society. Research (R&D) or other forms of knowledge production, which are university-based and firm-based, are linked together more in a first-then relationship. One career pattern in Mode 1, therefore, may be an academic researcher starts working at a university, leaves for a firm, and later may be interested in reentering the university. The world of Mode 2 universities is already more complicated. In Mode 2, quality is directed toward an efficient and/or effective problem-solving. The problem-solving is being evaluated by communities of knowledge producers as well as knowledge users. Thus the spectrum of potential peers in Mode 2 enlarges itself dramatically. Disciplinary-based peer review loses in Mode 2 its primary gate-keeping function. However, at the same time, defining criteria for quality or a quality-based selection of peers (coming from the knowledge producer and/or knowledge user side) may turn into an equally tricky proposition for Mode 2. *While Mode 2 knowledge is just as important as Mode 1 knowledge,* we might experience in higher education that the core faculty is being dominated by the Mode 1 knowledge paradigm and that Mode 2 knowledge paradigms are being pushed outward to the context of the noncore faculty. In higher education operates a potential mismatch between Mode 1 and Mode 2, to the disadvantage of Mode 2, even though for innovation it is so crucially important that higher education covers and integrates the comprehensive spectrum of knowledge production of Mode 1 and Mode 2. The Mode 3 knowledge paradigm, on the contrary, emphasizes that higher education institutions should reflect consciously on whether developing a Mode 1 or Mode 2 profile (portfolio), or Mode 1 *and* Mode 2, and what opportunities there exist for creatively combining Mode 1 and Mode 2. Mode 3 challenges universities but also liberates universities from a possible Mode 1 and Mode 2 deadlock, *encouraging and highlighting novel routes of quality enhancement for further development*. Implications may be manifold: (a) the same academic (core) faculty could be partially Mode 1 and Mode 2 based and (b) the nonlinear innovation momentum of Mode 3 suggests that academic workers should not necessarily engage first in basic university research and later in applied firm research but may do both at the same time. For this second option, we propose the term and concept of "cross-employment" or multi-employment (Campbell 2011). *Implications of this are that knowledge producers and R&D workers are being simultaneously employed by more than one organization or institution*. Several forms and variations of cross-employment are thinkable and reasonable. Cross-employment can stretch (in network-style arrangements) across different higher education institutions or can link universities with nonuniversities, i.e., organizations outside of higher

education (e.g., firms or organizations of the civil society). Civil society represents explicitly one reference for the Quadruple Helix innovation system, by this also co-constituting the Quadruple Helix (Carayannis and Campbell 2009, p. 207; 2011, 2012, pp. 13–14). Cross-employment should foster the creativity of and in knowledge production and knowledge creation. The cross-employed academic profession or cross-employed academic faculty involves itself and engages in a much broader spectrum of knowledge production, possibly integrating Mode 1 and Mode 2 knowledge and knowledge skills. *In a university, operating under Mode 3, the same academic faculty member could be based in parallel on different academic employment contracts that interplay.* This overlapping of employment contracts could help making the boundaries between core and noncore faculty more flexible, more open, and fairer. *Cross-employment enables the academic faculty and academic profession to engage in in-parallel "cross-careers" inside and outside of higher education at one and the same time*. The same knowledge-producing person can follow career tracks at two different universities or at a university and a nonuniversity organization. Cross-careers and cross-employment support the formation of (hybrid) networks between organizations and contribute to the networking capabilities and capacities of organizations. *Cross-employment facilitates and sustains nonlinear innovation.* This should add crucially to the dynamics of "self-organizing, cross-overlapping networks" (see again Fig. 2). *Cross-employment and cross-careers, in cross-connection to Mode 1, Mode 2, and Mode 3, certainly identify potential objectives for epistemic governance*. In final implication, cross-employment represents a role model of equal importance for academic (university) careers, when compared with the academic career model of tenure track. *Therefore, cross-employment is a role model for academic careers (inside and outside of higher education), on par with tenure track*. This we want to recognize as a proposition for further discussion. In pragmatic terms, of course, the empirical trend still would have to be verified: "It remains to be seen, whether cross-employment has the capability to establish itself as an additional and positively-defined role model for academic careers in higher education, in parallel to the already existing role mode of tenure-track (tenure)" (Carayannis and Campbell 2012, p. 26).

Conclusion

Epistemic governance and epistemic innovation policy formulate a critique against too-narrowly defined approaches to governance, where governance follows one-sidedly bureaucratic or technocratic considerations. Instead, epistemic governance (also quality management and quality enhancement) and epistemic innovation policy should be regarded as a plea for a more comprehensive understanding, where the explicit-making, comprehension and reflection of knowledge, knowledge production, and knowledge application are key for a successful governing and governance. In that respect, epistemic governance speaks and argues also in favor for the practical feasibility of a "Philosophy of Governance." Epistemic governance, as a

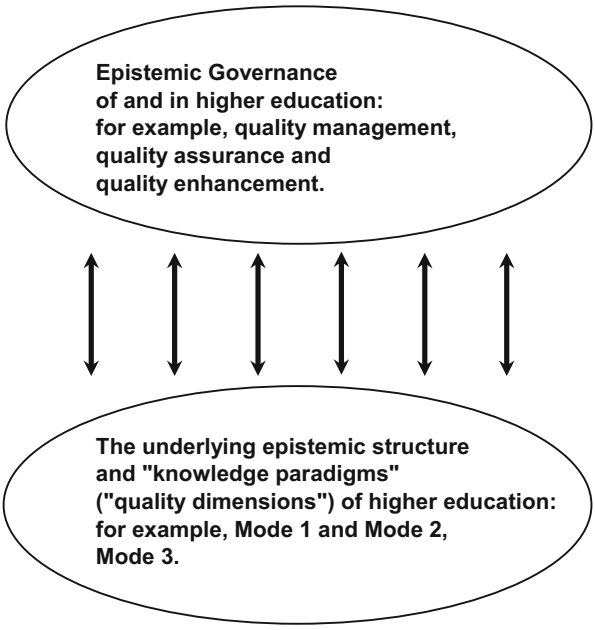


Fig. 3 Core model of epistemic governance of and in higher education (Source: Authors' own conceptualization based on Campbell and Carayannis (2013a, p. 28, b))

concept and as a practice, qualifies as a novel form of governance, representing a new and innovative frontier and frontier line of and for governance, with a hybrid overlapping to other concepts and measures such as network governance, cross-employment, and epistemic innovation policy (see Fig. 3 for the core model of epistemic governance of and in higher education). There is also a governance of innovation and innovation policy, so the cross-connections between epistemic governance and epistemic innovation policy demand further elaboration and a more advanced fine-tuning for practical purposes. In conceptual terms, epistemic governance and epistemic innovation policy still require to be broadened and expanded. For example, also universities of the arts are being regarded as institutions that contribute considerably to national and multilevel innovation systems (Carayannis and Campbell 2012, pp. 14–17). From that universities-of-arts-based input, important interdisciplinary and transdisciplinary impulses are ought to be expected. The specific and potential roles of arts universities and artistic research, also in connection to their governance and epistemic governance, are to be further developed. The same applies to cross-connections between artistic research, artistic innovation, and epistemic innovation policy. Knowledge economy, knowledge society, and knowledge democracy are being intertwined (on knowledge democracy, see also In't Veld 2010).

Cyber development can be defined as a development in terms of a sustainable development of knowledge economy, knowledge society, and knowledge democracy that is knowledge based and knowledge driven and where innovation is playing a crucial role. In this context, Epistemic Governance and Epistemic Innovation Policy within higher education and higher education systems, but also beyond higher

education and higher education systems, represent an understanding and a strategy that is crucial for governance and further progress and advancement in the knowledge economy that is being interlinked with knowledge society and knowledge democracy. We are experiencing here a new type of governance and a new set of policies.

Epistemic Governance innovates governance. Epistemic Governance innovates governance and innovation and innovation policy.

Cross-References

- ▶ Academic Firm in Cyber-Development: The New Design and Redesign Proposition for Entrepreneurship in the Innovation-Driven Knowledge Economy
- ▶ Quadruple and Quintuple Helix Innovation Systems and Mode 3 Knowledge Production
- ▶ Quality of Democracy in Quadruple Helix Structures: OECD Countries in Global Comparison

References

Arnold, M. (2009). Interdisziplinarität: Theorie und Praxis eines Forschungskonzepts. In M. Arnold (Ed.), *iff. Interdisziplinäre Wissenschaft im Wandel* (pp. 65–97). Vienna: LIT.

Bush, V. (1945). *Science: The endless frontier*. Washington, DC: United States Government Printing Office. http://www.nsf.gov/od/lpa/nsf50/vbush1945.htm#transmittal

Campbell, D. F. J. (2000). Forschungspolitische Trends in wissenschaftsbasierten Gesellschaften. Strategiemuster für entwickelte Wirtschaftssysteme. *Wirtschaftspolitische Blätter, 47*(2), 130–143.

Campbell, D. F. J. (2003). The evaluation of university research in the United Kingdom and the Netherlands, Germany and Austria. In P. Shapira & S. Kuhlmann (Eds.), *Learning from science and technology policy evaluation: Experiences from the United States and Europe* (pp. 98–131). Camberley: Edward Elgar.

Campbell, D. F. J. (2006). The university/business research networks in science and technology. Knowledge production trends in the United States, European Union and Japan. In E. G. Carayannis & D. F. J. Campbell (Eds.), *Knowledge creation, diffusion, and use in innovation networks and knowledge clusters. A comparative systems approach across the United States, Europe and Asia* (pp. 67–100). Westport: Praeger.

Campbell, D. F. J. (2011). Wissenschaftliche „Parallelkarrieren" als Chance. Wenn Wissenschaft immer öfter zur Halbtagsbeschäftigung wird, könnte eine Lösung im „Cross-Employment" liegen. Guest Commentary for DIE PRESSE (February 2, 2011). http://diepresse.com/home/bildung/meinung/635781/Wissenschaftliche-Parallelkarrieren-als-Chance?direct=635777&_vl_backlink=/home/bildung/index.do&selChannel=500

Campbell, D. F. J., & Carayannis, E. G. (2012). Lineare und nicht-lineare knowledge production: Innovative Herausforderungen für das Hochschulsystem. *Zeitschrift für Hochschulentwicklung, 7*(2), 64–72. http://www.zfhe.at/index.php/zfhe/article/view/448

Campbell, D. F. J., & Carayannis, E. G. (2013a). *Epistemic governance in higher education. Quality enhancement of universities for development. SpringerBriefs in business*. New York: Springer. http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6

Campbell, D. F. J., & Carayannis, E. G. (2013b). Epistemic governance and epistemic innovation policy, 697–702. In E. G. Carayannis (Editor-in-Chief), I. N. Dubina, N. Seel, D. F. J. Campbell, D. Uzunidis (Associate Editors) (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship*. New York: Springer. http://link.springer.com/referenceworkentry/10.1007/978-1-4614-3858-8_271

Campbell, D. F. J., & Güttel, W. H. (2005). Knowledge production of firms: Research networks and the "Scientification" of business R &D. *International Journal of Technology Management, 31* (1/2), 152–175. http://www.inderscience.com/search/index.php?action=record&rec_id=6629&prevQuery=&ps=10&m=or

Carayannis, E. G., & Campbell, D. F. J. (2006). "Mode 3": Meaning and implications from a knowledge systems perspective. In E. G. Carayannis & D. F. J. Campbell (Eds.), *Knowledge creation, diffusion, and use in innovation networks and knowledge clusters. A comparative systems approach across the United States, Europe and Asia* (pp. 1–25). Westport: Praeger.

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "Quadruple Helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46* (3/4), 201–234. http://www.inderscience.com/browse/index.php?journalID=27&year=2009&vol=46&issue=3/4 and http://www.inderscience.com/search/index.php?action=record&rec_id=23374&prevQuery=&ps=10&m=or

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69. http://www.igi-global.com/bookstore/article.aspx?titleid=41959

Carayannis, E. G., & Campbell, D. F. J. (2011). Open innovation diplomacy and a 21st century fractal research, education and innovation (FREIE) ecosystem: Building on the quadruple and quintuple helix innovation concepts and the "Mode 3" knowledge production system. *Journal of the Knowledge Economy, 2*(3), 327–372. http://www.springerlink.com/content/d1lr223321305579/

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development. SpringerBriefs in business*. New York: Springer. http://www.springer.com/business+%26+management/book/978-1-4614-2061-3

Danilda, I., Lindberg, M., & Torstensson, B.-M. (2009). Women resource centres. A quattro helix innovation system on the European agenda. Paper http://pure.ltu.se/portal/files/2806203/Danilda-Lindberg-Torstensson-paper.pdf

Dubina, I. N., Carayannis, E. G., & Campbell, D. F. J. (2012). Creativity economy and a crisis of the economy? Co-evolution of knowledge, innovation and creativity, and of the knowledge economy and knowledge society. *Journal of the Knowledge Economy, 3*(1), 1–24. http://www.springerlink.com/content/t5j8l12136h526h5/

Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation: From national systems and "mode 2" to a triple helix of university-industry-government relations. *Research Policy, 29*, 109–123.

Etzkowitz, H. (2003). Research Groups as "Quasi-Frims": The Invention of the Enterpreneurial University. *Research Policy, 2*, 109–121.

Ferlie, E., Musselin, C., & Andresani, G. (2008). The steering of higher education systems: A public management perspective. *Higher Education, 56*(3), 325–348. http://www.springerlink.com/content/n22v788851377144/fulltext.pdf

Ferlie, E., Musselin, C., & Andresani, G. (2009). The governance of higher education systems: A public management. Perspective. In C. Paradeise, E. Reale, I. Bleiklie, & E. Ferlie (Eds.), *University governance. Western european comparative perspectives* (pp. 1–20). Dordrecht: Springer.

Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P., & Trow, M. (1994). *The new production of knowledge. The dynamics of science and research in contemporary societies*. London: Sage.

Gottweis, H. (1998). Governing molecules. In *The discursive politics of genetic engineering in Europe and the United States*. Cambridge, MA: MIT Press.

Hemlin, S., Allwood, C. M., & Martin, B. R. (2004). *Creative knowledge environments. The influences on creativity in research and innovation*. Cheltenham: Edward Elgar.

Hindmarsh, R., & Prainsack, B. (Eds.). (2010). *Genetic suspects. Global governance of forensic DNA profiling and databasing*. Cambridge: Cambridge University Press.

In't Veld, R. J. (Ed.). (2010). *Knowledge democracy. Consequences for science, politics, and media*. Heidelberg: Springer. http://www.springer.com/de/book/9783642113802 and https://link.springer.com/book/10.1007%2F978-3-642-11381-9

Kuhn, T. S. (1962). *The structure of scientific revolutions*. Chicago: The University of Chicago Press.

Narin, F., Hamilton, K. S., & Olivastro, D. (1997). The increasing linkage between U.S. technology and public science. *Research Policy, 26*, 317–330.

Nowotny, H., Scott, P., & Gibbons, M. (2001). *Re-thinking science. Knowledge and the public in an age of uncertainty*. Cambridge: Polity Press.

Nowotny, H., Scott, P., & Gibbons, M. (2003). Mode 2 revisited: The new production of knowledge. *Minerva, 41*, 179–194.

Nowotny, H., Scott, P., & Gibbons, M. (2006). Re-thinking science: Mode 2 in societal context. In E. G. Carayannis & D. F. J. Campbell (Eds.), *Knowledge creation, diffusion, and use in innovation networks and knowledge clusters. A comparative systems approach across the United States, Europe and Asia* (pp. 39–51). Westport: Praeger.

Prainsack, B., & Wolinsky, H. (2010). Direct-to-consumer genome testing: Opportunities for pharmacogenomics research? *Pharmacogenomics, 11*(5), 651–655.

Scott, P. (2009). Markets and new modes of knowledge production. In J. Enders & E. de Weert (Eds.), *The changing face of academic life. Analytical and comparative perspectives* (pp. 58–77). London: Palgrave Macmillan.

Vadrot, A. B. M. (2011). Reflections on mode 3, the co-evolution of knowledge and innovation systems and how it relates to sustainable development. Conceptual framework for "Epistemic Governance". *International Journal of Social Ecology and Sustainable Development, 2*(1), 44–52. http://www.igi-global.com/bookstore/article.aspx?titleid=51636

5 The Role of Information and Communication Technology (ICT) in the Governance of Energy Access: Exploring Application of Quadruple and Quintuple Helix Innovation Theory in Technology Transfer

Matthias Galan, David F. J. Campbell, and Elias G. Carayannis

Contents

M. Galan (✉)
Amsterdam, Netherlands

Vienna, Austria
e-mail: matthias.galan@gmail.com

D. F. J. Campbell
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@aau.at; david.campbell@uni-ak.ac.at; david.campbell@univie.ac.at

E. G. Carayannis
Department of Information Systems and Technology Management, School of Business, The George Washington University, Washington, DC, USA
e-mail: caraye@gwu.edu

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_55

Abstract

Access to environment-friendly technologies is the key to enable the implementation of the newly adopted Sustainable Development Goals and especially goal number seven to "ensure access to affordable, reliable, sustainable, and modern energy for all." It remains an issue that the transfer of such technologies is highly politicized. This analysis wants to explore the applicability of Quadruple and Quintuple Helix Theory to the global concern of sustainable development and especially to the quest for energy access. We would like to look for potential avenues to better understand the innovative momentum of ongoing global change and implications for quality of democracy by looking at the potential of information and communication technology (ICT) in making environmentally sound technologies even more viable solutions for energy transition.

Keywords

Energy access · Energy poverty · Enernet · Ghana · Governance · ICT (information and communication technology) · Innovation · Public-civil society-private partnerships · Public-private partnerships · Quadruple and quintuple helix innovation systems · Sustainable development · Technology transfer

Introduction and Scope of This Chapter

This chapter wants to explore the applicability of Quadruple and Quintuple Helix Theory in overcoming global concerns such as climate change or energy poverty. We believe that with the adoption of the Sustainable Development Goals in 2015, increased attention needs to be put on the innovative potential of renewable energy technology in combination with ICT (information and communication technology) and ICT-based services in the context of access to energy in developing countries. Therefore, we would like to look for potential avenues for understanding the innovative momentum of ongoing global change and implications for quality of democracy. We will therefore look at the Quadruple and Quintuple Helix Innovation Theory as developed in the literature (see Campbell et al. 2015; Carayannis et al. 2012; Campbell and Carayannis 2012; Carayannis and Campbell 2010; Carayannis and Campbell 2009).

This analysis aims to explore empirical implications of applying Quadruple and Quintuple Helix Theory. We want to focus our exploration on renewable energy and related ICT-based services as an innovative solution for energy poverty in developing countries.

Energy represents a technology field that has transformed into a field of crucial importance for further innovation and development. "Energy is the new new

internet." "Today, the actors are SolarCity, Sunrun and a host of others moving us off fossil fuels and into clean energy supported by smart equipment, services and software, offered atop existing utility networks. This time, it's the enernet." The term and concept of the *enernet* is being defined as: "A dynamic, distributed, redundant and multi-participant energy network built around clean energy generation, storage and delivery and serving as the foundation for smart cities" (Lakamp 2017, pp. 1–2). The concept of enernet bridges and brings together explicitly (and metaphorically) energy and ICT.

When moving the inquiry on innovation away from the often bilateral context of innovation cooperation and into a global governance perspective of innovation, a decisive increase of complexity has to be taken into account (Rosenau develops the concept of fragmegration to describe the "complex puzzle" that governance in a complex world has become. The term is meant to describe the "simultaneity and interaction of the fragmenting and integrating dynamics that are giving rise to new spheres of authority and transforming the old spheres" (Rosenau 1997, p. 38)). As Rosenau explains, this is a complex challenge to scholars: "In short, we live in and study a fragmegrative world that often cascades events through, over, and around the long established boundaries of states and, on some occasions, relocates authority outwards to transnational, and supranational organizations, sidewards to social movements and NGOs, and inwards to subnational groups.[...] It is a world in which the logic of governance does not necessarily follow hierarchical lines, in which what is distant is also proximate, and in which the spacial and temporal dimensions are so confounded by fragmegrative dynamics as to rid event sequences of any linearity they may once have had" (Rosenau 1997, p. 43, 44).

First (Section "Origins of the Quadruple and Quintuple Helix Model of Innovation"), we will depict the discourse on Quadruple and Quintuple Helix Innovation Theory and how it connects to sustainable development. In a *second* step (Sections "Governance of Energy Access" and "Technology Transfer: The International Perspective"), we will look at the governance of energy access in a global perspective. In a *third* step (Section "The empirical Challenge: ICT and Renewable Energy in Perspective"), we will look at the role of ICT-based services in redefining the framework of energy access. This will be done by looking into the application of ICT to improve energy access in the renewable energy sector and the role of public-private partnerships in facilitating energy access in the context of sub-Saharan African countries. In a *fourth* and final step, we want to conclude with takeaways of the role of ICT in reshaping energy access through renewable energy sources and look at the implications for Quadruple and Quintuple Helix Innovation Theory.

Origins of the Quadruple and Quintuple Helix Model of Innovation

The Quadruple and Quintuple Helix Innovation Theory focuses on the cross-linkages, cross-references, and co-evolution of knowledge economy, knowledge society, and knowledge economy in the context of environment and social ecology. This innovation theory develops a progressive vision of development in society,

democracy, and economy; emphasizes the qualities of sustainable development; and understands knowledge (knowledge production, knowledge creation) to be essential for innovation (knowledge application, knowledge use) in innovation systems. The Quadruple and Quintuple Helix Innovation Theory has interwoven the ideas of Mode 1, Mode 2, Mode 3, and Triple, Quadruple, and Quintuple Helix. We will now describe the evolution that led to the development of this theory of innovation.

At the beginning, the concept of university research has been at the center of innovation research. A traditional understanding of innovation referring to universities in the sciences focuses on basic research, often framed within a matrix of academic disciplines, and without a particular interest in the practical use of knowledge and innovation. This model of university-based knowledge production is also being called "Mode 1" of knowledge production (Gibbons et al. 1994). Mode 1 is also compatible with the linear model of innovation, which is often being referred to by Vannevar Bush (1945). The linear model of innovation asserts that first there is basic research in university context; gradually, this university research will diffuse out into society and the economy. It is then the economy and the firms that pick up the lines of university research, and develop these further into knowledge application and innovation, for the purpose of creating economic and commercial success in the markets outside of the higher education system. Within the frame of linear innovation, there is a sequential "first-then" relationship between basic research (knowledge production) and innovation (knowledge application).

The Mode-1-based understanding of knowledge production has been challenged by the new concept of "Mode 2" of knowledge production, which was developed and proposed by Michael Gibbons et al. (1994, pp. 3-8, 167). Mode 2 emphasizes a knowledge application and a knowledge-based problem-solving that involves and encourages the following principles: "knowledge produced in the context of application"; "transdisciplinarity"; "heterogeneity and organizational diversity"; "social accountability and reflexivity"; and "quality control" (see furthermore Nowotny et al. 2001, 2003, 2006). Key in this setting is the focus on a knowledge production in contexts of application. Mode 2 expresses and encourages clear references to innovation and innovation models. The linear model of innovation also has become challenged by nonlinear models of innovation, which are interested in drawing more direct connections between knowledge production and knowledge application, where basic research and innovation are being coupled together not in a first-then, but in an "as well as" and "parallel" (parallelized) relationship (Campbell and Carayannis 2012). Mode 2 appears also to be compatible with nonlinear innovation and its ramifications.

The Triple Helix model of knowledge, innovation, and university-industry-government relations, which was introduced and developed by Henry Etzkowitz and Loet Leydesdorff (2000, pp. 111–112), asserts a basic core model for knowledge production and innovation, where three "helices" intertwine, by this creating a national innovation system. The three helices are identified by the following systems or sectors: academia (universities), industry (business), and state (government). Etzkowitz and Leydesdorff refer to "university-industry-government relations" and networks, putting a particular emphasis on "tri-lateral networks and hybrid organizations," where those helices overlap in a hybrid fashion. Etzkowitz and Leydesdorff (2000, p. 118) also explain how, in their view, the Triple Helix model relates to Mode

2: the "Triple Helix overlay provides a model at the level of social structure for the explanation of Mode 2 as an historically emerging structure for the production of scientific knowledge, and its relation to Mode 1." More recently, Leydesdorff (2012) also introduced the notion of "N-Tuple of Helices."

Mode 1 and Mode 2 may be characterized as "knowledge paradigms" that underlie the knowledge production (to a certain extent also the knowledge application) of higher education institutions and university systems. Success or quality, in accordance with Mode 1, may be defined as: "*academic excellence, which is a comprehensive explanation of the world (and of society) on the basis of 'basic principles' or 'first principles', as is being judged by knowledge producer communities (academic communities structured according to a disciplinary framed peer review system).*" Consequently, success and quality, in accordance with Mode 2, can be defined as: "*problem-solving, which is a useful (efficient, effective) problem-solving for the world (and for society), as is being judged by knowledge producer and knowledge user communities*" (Campbell and Carayannis 2013a, p. 32). A "Mode 3" university, higher education institution or higher education system, would represent a type of organization or system that seeks creative ways of combining and integrating different principles of knowledge production and knowledge application (e.g., Mode 1 and Mode 2), by this encouraging diversity and heterogeneity and also creating creative and innovative organizational contexts for research and innovation. Mode 3 encourages the formation of "creative knowledge environments" (Hemlin et al. 2004). "Mode 3 universities," Mode 3 higher education institutions and systems, are prepared to perform "basic research in the context of application" (Campbell and Carayannis 2013a, p. 34). This has furthermore qualities of nonlinear innovation. Governance of higher education and governance in higher education must also be sensitive, whether a higher education institution operates on the basis of Mode 1, Mode 2, or a combination of these in Mode 3. The concept of "epistemic governance" emphasizes that the underlying knowledge paradigms of knowledge production and knowledge application are being addressed by quality assurance and quality enhancement strategies, policies, and measures (Campbell and Carayannis 2013a, b, 2016).

Emphasizing again a more systemic perspective for the Mode 3 knowledge production, a focused conceptual definition may be as follows (Carayannis and Campbell 2012, p. 49): Mode 3 "... allows and emphasizes the co-existence and co-evolution of different knowledge and innovation paradigms. In fact, a key hypothesis is: The competitiveness and superiority of a knowledge system or the degree of advanced development of a knowledge system are highly determined by their adaptive capacity to combine and integrate different knowledge and innovation modes via co-evolution, co-specialization and co-opetition knowledge stock and flow dynamics" (see Carayannis and Campbell 2009; on "Co-Opetition," see Brandenburger and Nalebuff 1997). Analogies are being drawn and a co-evolution is being suggested between diversity and heterogeneity in advanced knowledge society and knowledge economy, and political pluralism in democracy (knowledge democracy), and the quality of a democracy. The "Democracy of Knowledge" refers to this overlapping relationship. As is being asserted: "The *Democracy of Knowledge*, as a concept and metaphor, highlights and underscores parallel processes between

political pluralism in advanced democracy, and knowledge and innovation heterogeneity and diversity in advanced economy and society. Here, we may observe a hybrid overlapping between the *knowledge economy, knowledge society and knowledge democracy*" (Carayannis and Campbell 2012, p. 55). The "Democracy of Knowledge," therefore, is further reaching than the earlier idea of the "Republic of Science" (Michael Polanyi 1962).

The main focus of the Triple Helix innovation model concentrates on university-industry-government relations (Etzkowitz and Leydesdorff 2000). In that respect, Triple Helix represents a basic model or a core model for knowledge production and innovation application. The models of the Quadruple Helix and Quintuple Helix innovation systems are designed to comprehend already and to refer to an extended complexity in knowledge production and knowledge application (innovation); thus, the analytical architecture of these models is broader conceptualized. To use metaphoric terms, the Quadruple Helix embeds and contextualizes the Triple Helix, while the Quintuple Helix embeds and contextualizes the Quadruple Helix (and Triple Helix). The Quadruple Helix adds as a fourth helix the "media-based and culture-based public," the "civil society," and "arts, artistic research and arts-based innovation" (Carayannis and Campbell 2009, 2012, p. 14; see also Danilda et al. 2009; furthermore, see Carayannis and Campbell 2017 and Monteiro et al. 2017). The Quadruple Helix also could be emphasized as the view and perspective that specifically brings in the "dimension of democracy" or the "context of democracy" for knowledge, knowledge production, and innovation. The Quintuple Helix innovation model is even more comprehensive in its analytical and explanatory stretch and approach, adding furthermore the fifth helix (and perspective) of the "natural environments of society" (Carayannis and Campbell 2010, p. 62). Within the Quadruple and Quintuple Helix Innovation Theory approach, networking is important, adding to the public-private partnerships also the angle of *public-civil society-private partnerships*, which are becoming key for the support of governance and governance system initiatives.

The Triple Helix is explicit in acknowledging the importance of higher education for innovation. However, it could be argued that the Triple Helix sees knowledge production and innovation in relation to economy, thus the Triple Helix models, first of all (primarily), the economy and economic activity. In that sense, the Triple Helix frames the knowledge economy. The Quadruple Helix brings in the additional perspective of society (knowledge society) and of democracy (knowledge democracy). The Quadruple-Helix-innovation-system understanding emphasizes that sustainable development of and in economy (knowledge economy) requires that there is a co-evolution of knowledge economy, knowledge society, and knowledge democracy. The Quadruple Helix even encourages *the perspectives of knowledge society and of knowledge democracy* for supporting, promoting, and advancing knowledge production (research) and knowledge application (innovation). Furthermore, the Quadruple Helix is also explicit that not only universities (higher education institutions) of the sciences but also universities (higher education institutions) of the arts should be regarded as decisive and determining institutions for advancing next-stage innovation systems: the inter-disciplinary and trans-disciplinary connecting

of sciences and arts creates crucial and creative combinations for promoting and supporting innovation. Here, in fact, lies one of the keys for future success. The concept and term of "social ecology" refer to "society-nature interactions" between "human society" and the "material world" (see, e.g., Fischer-Kowalski and Haberl 2007). The European Commission (2009) identified the necessary socio-ecological transition of economy and society as one of the great next-phase challenges, but also as an opportunity, for the further progress and advancement of knowledge economy and knowledge society. The Quintuple Helix refers to this socio-ecological transition of society, economy, and democracy, the Quintuple Helix innovation system is therefore ecologically sensitive. Quintuple Helix bases its understanding of knowledge production (research) and knowledge application (innovation) on social ecology. Environmental issues (such as global warming) represent issues of concern and of survival for humanity and human civilization. But the Quintuple Helix translates environmental and ecological issues of concern also in potential opportunities, by identifying them as possible drivers for future knowledge production and innovation (Carayannis et al. 2012). This, finally, defines also opportunities for the knowledge economy. "The Quintuple Helix supports here the formation of a win-win situation between ecology, knowledge and innovation, creating synergies between economy, society and democracy" (Carayannis 2012, p. 1).

The following figure (Fig. 1) summarizes again visually the multilevel architecture of Quadruple and Quintuple Helix Innovation Theory (see also Carayannis and Campbell (2014) for more particulars).

State-Centric Dimensions of a Quadruple and Quintuple Helix Model of Innovation and Global Problem-Solving

As we have seen in the previous section, benchmarks developed in Quadruple and Quintuple Helix Innovation Theory can help to determine policy and strategy that leverages knowledge and innovation for long-term sustainable development

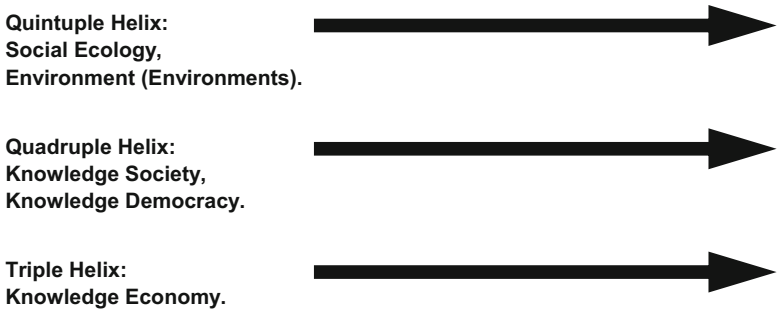


Fig. 1 The multilevel helix structure of innovation and innovation systems (Source: Author's own conceptualization based on Carayannis and Campbell (2009, p. 207; 2010, p. 62; 2014; 2017, p. 7), Carayannis et al. (2012, p. 4), Etzkowitz and Leydesdorff (2000, p. 112), Danilda et al. (2009))

in knowledge economy, knowledge society, and knowledge democracy. They also contribute to the work of entrepreneurs and firms, public decision-makers, and governments. Furthermore, Quadruple and Quintuple Helix Innovation Theory also brings civil society (and public-*civil society*-private partnerships) into perspective.

As Carayannis et al. point out, quadruple and quintuple helix models of innovation need to be understood as a "network-style linkage of knowledge." In their understanding, it is the (nation-)state which is the foundation for network-based innovation. They continue that this model challenges our understanding of a hegemonic (nation-)state in so far as it introduces sustainable development as another key indicator besides a strong leadership in world politics and economy. This new "dimension" could in their view assess the "social (societal) potential to balance new knowledge, know-how, and innovation with nature." (Carayannis et al. 2012, 3ff.)

In our view, the Quadruple and Quintuple Helix Innovation Theory can go beyond traditional analysis of champions of innovation in the OECD world and allows looking at networks spanning developed and developing countries. Therefore, we want to explore how potential avenues of Quadruple and Quintuple Helix Innovation Theory can be understood in such a context.

We see innovation beyond the nation-state in terms of global problem formulation and solving. As Carayannis and Kaloudis argue, "it is clear that the challenge of global warming is accompanied with the challenge of sustainability (for the world) in the twenty-first century." As global warming is therefore the single most important problem to be solved, we need to understand in which areas innovation has to take place in order to bring balance to our climate. In accordance with Carayannis and Kaloudis, we want to break global warming down into nine areas that require sustained action and intelligent use of technology: financial/economic system; environmental challenges; feed and heal the world challenges; energy challenges; educational challenges,; political democratic reform across the world; transformative government across the world; equity and security across the world; technology, innovation, and entrepreneurship as drivers of knowledge societies (Carayannis and Kaloudis 2010, p. 2).

We want to explore the area of energy challenges, which is particularly interesting as it transgresses most if not all of the described areas. Due to ongoing innovation in the sector such as the rise of renewable energy, a better understanding of existing policy frameworks for energy access and governance is necessary to better understand innovation (see Van de Graaf and Colgan 2016). The growing importance of energy challenges is also acknowledged in the Sustainable Development Goals (SDGs). Goal number seven defines affordable, reliable, sustainable, and modern energy for all as a goal for 2030. This also includes an increase of the share of renewable energy in the global energy mix and improvement in energy efficiency. The goal shall be reached by enhancing "international cooperation to facilitate access to clean energy research and technology, including renewable energy, energy efficiency and advanced and cleaner fossil-fuel technology, and promote investment in energy infrastructure and clean energy technology." Furthermore, it is stated that infrastructure and upgraded technology for supplying modern and sustainable

energy services shall be available for all in developing countries and in particular "least developed countries, small island developing states and landlocked developing countries, in accordance with their respective programmes of support" (UN 2015, p. 19).

Especially knowledge/technology transfer is an interesting topic from an innovation theory perspective. How can the knowledge about how to set up "infrastructure and upgraded technology for supplying modern and sustainable energy services" (UN 2015, p. 19) be made accessible for developing countries, when this touches upon key assets within the knowledge economy?

Within the framework of a Quadruple and Quintuple Helix model, this can be understood through the interplay of actors. Here, it is especially the helice of sustainable development which refers to the predominant issues of modern-day society. As this innovation model was developed to describe innovation in already stratified societies, we would like to see how the model can be used to describe innovation in a global context of sustainable development focusing on the developing world. This makes a thorough understanding of how actors involved in national innovation systems – academia, industry, government (see Etzkowitz and Leydesdorff 2000) – interact on a global level. Therefore, we would like to look at insights from global governance in the following section that we consider to be instructive in describing cooperation in global energy governance (GEG) and allowing to better understand the empirical and theoretical challenges in applying Quadruple and Quintuple Innovation Theory to a global setting.

Going Beyond the (Nation-)State

So far, explorations of how to apply Quadruple and Quintuple Helix Innovation Theory to the context of international cooperation have been based on the evaluation of bilateral cooperation. Casaramona et al. focus their investigation on the framework of the EUs cooperation with Mediterranean countries. The focus of their study clearly lies upon the cooperation within the setting of academia, industry, and government as defined in the Quadruple Helix framework. They focus on the mode of knowledge transfer in the renewable energy sector with, especially, North-African countries (Casaramona et al. 2015).

In their effort "to better understand the elements of successful knowledge transfer in order to create a model for a suitable environment for knowledge exploitation in the context of the international cooperation" they identify several hurdles:

> [T]he main hurdles to the setting up of an innovation-friendly ecosystem can be hereinafter summarized: (a) cultural aspects, including innovation culture; (b) rigid administrative and regulatory framework in the Mediterranean area (it is often considered rigid and unclear, too bureaucratic with consequence in researchers' behaviours with external actors); (c) researchers' mobility obstacles; (d) complex and not recognized patent exploitation procedures and IPR process and (e) lack of smart specialization strategies. These factors are able to affect the research and innovation activities, the technology transfer model and its adaptation in different geographical areas. (Casaramona et al. 2015, p. 505, 506)

The setting of Casaramona et al. focuses on researcher interactions in the context of the EUs cooperation with Mediterranean countries. The area of knowledge/technology transfer touches upon the transfer in the renewables sector, and the study aims to understand how knowledge transfer can work the best. On the following pages we would like to explore how these obstacles in this approach of knowledge transfer could be relevant in the analysis of renewable energy and ICT-based services in sub-Saharan Africa.

As Stamm et al. argue "global challenges call for co-operation on a global scale in order to create a public good or protect the global commons." Discussing the case of governance in science, technology, and innovation, they cite the example of a stable climate as one example for a global public good that is endangered by the actions of individuals and societies. Such "tragedy of the commons" (Hardin 1968) is in their view detrimental to the management of global public goods as each actor tries to get most out of an accessible resource. The authors argue that "effective governance mechanisms can help to deal with this problem." They continue that "in most cases, single governments cannot ensure effective solutions, and internationally co-ordinated action and collaboration are required. This does not necessarily imply the need for the entire world community to agree on joint action" (Stamm et al. 2012, p. 26, 27).

This is to say that international cooperation is crucial in order to get to terms with solutions for global issues. But as Stamm et al. also state, "governance mechanisms to address global challenges depend on the characteristics of the specific challenge, its urgency, the causative factors, the actors involved and their specific interests, power relations, etc. There is no simple formula. [. . .] Most problems faced by global governance institutions and processes in other areas, such as incentives to be uncooperative (prisoner's dilemma) and free-riding, apply equally to international science technology innovation (STI) cooperation. The temptation to benefit from the efforts of others (free-ride) is strong. If some actors invest to find solutions to global challenges, those that do not may still reap the benefits" (Stamm et al. 2012, p. 26, 27).

In order to apply the Quadruple and Quintuple Helix Model of innovation to a context of global governance, we have to keep in mind that we cannot see global issues only within the confounds of the nation-state. This makes it necessary to move beyond this setting and brings us back to the nine areas that require "sustained action" and "intelligent use of technology" according to Carayannis and Kaloudis 2010. Especially, energy challenges require sustained action and intelligent use of technology on a global scale in order to assure a balance in the helice of sustainable development. As Casaramona et al. argue, there are obstacles in the way of the necessary technology transfer that can enable such a balance in the helice of sustainable development.

Governance of Energy Access

In this section, we will define how the notion of energy challenges can be understood in the context of global governance. To do so, we will draw on the growing body of literature of global energy governance (GEG) to have an understanding of the

political framework in which innovation takes place. Here, we will identify how energy challenges can be understood in the context of global energy governance (see Biermann et al. 2009; Dubash and Florini 2011; Pattberg and Widerberg 2014; Van de Graaf and Colgan 2016).

As we have already seen in the discussion around SDG number seven, there is a very broad conception of what energy policy is and can achieve. Interestingly, it is only for a short time that global governance scholars and policy analysts are working on understanding energy governance beyond the national level (Dubash and Florini 2011, p. 6). Global energy governance has been "relatively unexplored in the literature, in part because it is hard to conceptualize as a coherent field" (ibid., p. 7). They continue that "[h]istorically, energy governance at both national and global scales has been fragmented by energy source – nuclear, oil and gas, coal, renewables and so on. In addition, energy is closely intertwined with the historical evolution of industrialization, and is a critical input to productive activity and social outcomes such as health, education and habitats. Finally, the consumption of energy comes with pervasive and persistent local and global externalities, notably climate change. All these aspects of energy use are studied, but it is daunting to consider the various interconnections within a single rubric" (ibid.)

The critical review concludes by pointing out that "the achievements of global energy governance fall far short of any reasonable assessment of a good outcome. Global energy governance consists of inadequate and uncoordinated mechanisms attempting to achieve fragmented and unprioritized objectives which pose as yet unresolved structural trade-offs. We do not currently have the institutional infrastructure needed to address the significant and urgent challenges we face" (ibid., p. 15).

Four objectives of energy governance are identified in the existing literature by Dubash and Florini. These are *energy supply security* which is the strategic aim of governments to secure energy access, *energy poverty* being the lack of access to energy necessary for human development, *environmental sustainability* which comprises pollution caused by the current way of gaining and consuming energy which again manifests in phenomena such as climate change, and finally *domestic good governance and corruption* (Dubash and Florini 2011, p. 7–11).

In a similar manner as Dubash and Florini, Van de Graaf and Colgan look at the emergent Global Energy Governance, (see Goldthau 2013). They identify "at least five major objectives" that are pursued by international organizations to a varying degree in conjunction with state and non-state actors. These objectives are depicted in a table that is reproduced in Table 1 (Van de Graaf and Colgan 2016, p. 3, 4).

The authors continue to explain that "[t]hese objectives form a part of GEG because they are associated with transboundary issues in one of three ways. First, some objectives, like managing global climate change or nuclear terrorism, clearly relate to the cross-border externalities of energy production and use. They exhibit global public goods characteristics and hence require action beyond the national level to avoid the collective action dilemmas associated

Table 1 Key goals of GEG and ways to achieve them (as proposed by Van de Graaf and Colgan 2016)

Goal	*Associated activities*
1. Security of energy supply and demand	Managing petroleum reserves to buffer energy shocks (e.g., coordinating releases from the IEA member states' strategic petroleum reserves) Energy market information sharing (e.g., Joint Organizations Data Initiative) and analysis (e.g., World Energy Outlook) Addressing pipeline politics and transit route disputes (e.g., Russia–Ukraine gas disputes) Managing long-term investment issues
2. Economic development	Reducing energy poverty (e.g., rural electrification programs) Facilitating technology transfer and cooperation (e.g., energy efficiency programs, nuclear technology sharing) Managing long-term investment profitability and macroeconomic stability
3. International security	Reducing the risk of nuclear proliferation, nuclear terrorism, and civilian nuclear accidents Addressing the links between oil, international arms purchases, and warfare Addressing sea piracy that targets oil and natural gas tankers Reducing and mitigating terrorist attacks on pipelines and energy infrastructure (including cyberattacks)
4. Environmental sustainability	Facilitating cooperation on global climate change Developing renewable energy sources, markets, and regulations Managing national and regional pollution deriving from energy production Facilitating carbon pricing policies
5. Domestic good governance	Addressing human rights violations associated with extractive industries Helping governments adopt rational, best-practices in regulation Encouraging transparency in energy markets and governance

Source: Van de Graaf and Colgan 2016, p. 4

with such goods." [. . .] "Second, other objectives, such as protecting human rights or reducing energy poverty, principally relate to individuals within national borders, but elicit concern and problem-solving (or problem-causing) action from international sources." [. . .] "Third, some objectives are international because states use international institutions to learn from, and/or cajole, each other to make changes to their domestic governance. Thus domestic good governance fits in the scope of GEG to the extent that actors seek to use international energy institutions to 'reach in' to areas of traditional sovereignty, typically in noncoercive ways such as best-practice sharing and information dissemination" (Van de Graaf and Colgan 2016, p. 4).

The five key goals reflect the state of discussions about Global Energy Governance. At the same time, it becomes clear that it is necessary to have a clear idea about which of these goals should be addressed by academic analysis. This becomes even more important in our case, as we are striving to connect the Quadruple and Quintuple Helix Innovation Theory with the global level.

Technology Transfer: The International Perspective

We will now turn to an analysis of technology transfer literature. An extensive body of literature discusses technology transfer and innovation. A recurrent motive is the role that private, public, and civil society actors should play in enabling this access. Related to the involvement of non-state actors, a group of authors claim that there is a need to better understand the national and local context of technology transfer and key players (see Haselip et al. 2015; de Coninck and Puig 2014). Some authors see Intellectual Property Rights (IPR) as a central issue, when it comes to technology transfer (see Abdel-Latif 2015; Shugurova and Shugurov 2015) There is limited satisfaction with the efficiency and success of international initiatives including multiple stakeholders, which affects the technology transfer (see Pattberg and Widerberg 2016; Haselip et al. 2015; de Coninck and Puig 2014).

The role of business interest in enabling the transfer of renewable energy technology is widely discussed. While some authors criticize the involvement of the private sector in decision-making and implementation, the predominant hardware focus in technology transfer and the market focus of technology transfer (see Haselip et al. 2015); others see a bigger involvement of business in decision-making as the key to establish market-based voluntary regimes. As Andrade and de Oliveira argue, this helps to hold the private sector accountable (see Andrade and de Oliveira 2015).

Another area of analysis is related to the outcomes of technology transfer and measures to improve them. Several authors look at the impact international institutions have made in promoting technology transfer of climate change mitigation technology (see de Coninck and Puig 2014; Pueyo and Linares 2012) De Coninck and Puig argue that there has been some success, but there needs to be more attention towards the role of users, governments, and universities. It is the role of information on environmentally sound technologies (ESTs) in a local context that they see as important to guarantee a broader success (see de Coninck and Puig 2014). Pattberg and Widerberg look at the lessons to be learned from the current transnational multistakeholder approach in global environmental governance. They address a widespread concern that there is little efficiency in this approach and propose nine recommendations for improvement (see Pattberg and Widerberg 2016).

The role of Intellectual Property Rights (IPR) in the UNFCCC negotiations reflects the stalemate in the broader debate about IPR in other fora such as the WTO. This unsolved issue is discussed by Abdel-Latif, who argues that it creates many challenges and issues for the dissemination of renewable energy technologies. He describes the role of IPR in UNFCCC negotiations and related disputes. He argues that these discussions will become more important in the future, making a more structured debate necessary (see Abdel-Latif 2015). Shugurova and Shugurov confirm the increased importance of IPR in debates around multilateral environmental agreements (MEAs) and see this as a particular challenge for international environmental law (See Shugurova and Shugurov 2015).

As we can see from this literature review and findings by Casaramona (Casaramona et al. 2015), technology transfer and IPR are closely related to the success of economic development. Here, the question is how said transfer of, in our

case, renewable energy technology takes place. When understanding the transfer in the actor framework of governments, industry, and academia, who should be in the driving seat and which problems arise from the structure of transfer. In the following section, we will look at market-based approaches of technology transfer based on public-private cooperation.

The Empirical Challenge: ICT and Renewable Energy in Perspective

In this section, we will discuss empirical implications of ICT and renewable energy in the context of developing countries focusing on sub-Saharan Africa. We will look at the case of energy poverty in this setting and discuss initiatives in providing energy to people living beyond the power grid.

The International Energy Agency (IEA) states that there were 1.3 billion people in 2010 who did not have access to electricity. It is an overall 2.6 billion people around the globe who were relying on biomass for cooking. This lack of energy access especially affects rural areas in the developing countries of Asia and sub-Saharan Africa, where electrification rates are only at about 64% (IEA 2012, p. 532, 533).

These numbers show that it will need considerable effort to reach the goal of universal energy access by 2030. The ambitious target was defined by the United Nations (UN) back in 2012, which was the UN year of "Sustainable Energy for All." For that purpose, the Sustainable Energy for All initiative (SE4All) was launched. In this framework, public and private actors as well as civil society organizations shall cooperate to ensure success. The goal of making energy access sustainable is seen as a way of, at the same time, eradicating poverty and decreasing CO_2 emissions, while creating new economic and social opportunities (SE4All 2014, p. 4).

As this shows we face a complex "puzzle" (puzzle is understood as a "genuine puzzle, the kind that is not easily answered but that is sufficiently engaging to linger, agitate, or otherwise sustain motivation in the face of continuous frustrations over the elusiveness of the answer" (see Rosenau 1997, p. 14) which combines insights from environmental, development, and trade debates. It has to be understood through the interaction of a variety of actors, governance levels, and processes that in their interrelation express an underlying power structure defining the shape of energy access and giving insights to the fate of the ambitious goal of universal energy access. In this section, we will analyze the relation of ICT and renewable energy in the context of the fight for access to energy.

ICT and Development

According to the latest Global Internet Report, it is especially mobile technologies which help to overcome the global digital divide and allow people in remote areas to access the Internet. Three key figures are important in this regard. The report states that 94% of the world's population can receive a mobile telephone signal, at the same

time 50% of the world's population can receive a mobile internet signal, because a mobile network can be upgraded to offer Internet with far less investment than building the original network. Finally, 36% of the population has subscribed to the mobile Internet in just 6 or 7 years, when mobile services were introduced. This is due to the wide availability of smartphones with millions of apps today (Internet Society 2016).

Despite these very high numbers, the report also states that there are big regional variations. In developed Asia Pacific, 99% of the population has a 3G signal, and 109% have a subscription – some have even more than one. The situation is a lot different in sub-Saharan Africa, where 82% of the population has a mobile signal, 35% have a 3G signal, but only 11% have subscribed to mobile Internet (Internet Society 2016).

The take-away from these numbers is that in all regions availability of the Internet is no longer the limiting factor. Mobile Internet is always available to many more people than have actually adopted it, and can grow relatively easily to cover the entire mobile network if needed. Therefore, the key question according to the Global Internet Report is why potential users who could access a service have not done so. On the one hand, affordability plays a crucial role as broadband costs range around 10% of the average monthly income, but it is also relevance that has to be considered. Relevance depends on the availability of apps in local language, interest, and usefulness to the consumers (Internet Society 2016).

Hanna argues that the ongoing ICT revolution, combined with the forces of globalization, "has provoked intense hopes and fears in countries at all levels of development. The hope is to leapfrog to a fast-paced, knowledge-based, innovation-driven, and networked economy. The fear is to be kept out of the knowledge and learning loop, fail to surf the wave of change and perhaps to be left irremediably behind, unable to catch the next wave. Others remain sceptical or concerned but have not adopted any coherent response, perhaps overwhelmed by day-to-day development challenges" (Hanna 2010, p. 2).

Hanna defines three fundamental roles that ICT can play in the context of cyber development and especially developing countries:

- "Accessing and processing information and knowledge, with dramatic increase in the power and speed to access, process, adapt, and organize information. This, in turn, has accelerated learning, innovation, and knowledge creation and dissemination. In this sense, ICT may have at least the same profound impact of the invention of the printing press and mass media."
- "Speeding up and reducing the costs of production and transactions throughout the economy. ICT is increasingly embedded into all types of production, processes, and transactions, giving rise to intelligent products, real-time control processes, facilitating trade, outsourcing business support and back-office services, and enabling complementary organizational innovations. In this sense, ICT may have similar implications as the steam engine, the electricity, and the railways in transforming production and transportation systems."

- "Making connections among people, NGOs, enterprises, and communities. This gives rise to empowerment, participation, coordination, decentralization, social learning, connecting communities of practice, mobilizing social capital, and globalizing civil society concerns. ICTs have been increasingly described as 'technologies of freedom'. There may not be a historical parallel to the enabling role of ICT to coordinate, collaborate, and empower" (Hanna 2010, p. 80).

Reflecting on these three fundamental roles, Hanna concludes that "[r]ather than treating ICT as an isolated sector on its own, ICT should be used as a lens to rethink development strategies, as a tool to enable all sectors and as a new and powerful means to empower the poor. This does not mean that we believe in ICT as a technology fix, but that an understanding of the full potential and implications of the ongoing technological revolution is necessary to realize its potential for development—far beyond its contribution as a sector. It is also essential to understand what makes ICT different from other technologies or from earlier technological revolutions in order to marshal the specific policies, institutions, and capabilities (and their complementarities) that must accompany the effective use of ICT as an enabler for development" (Hanna 2010, p. 81).

Furthermore, it is the political economy that needs to be understood to improve governance, policies, and institutions. This is fundamental to enable "a broad transformation to an inclusive broad transformation to an inclusive knowledge economy and information society." In order to do so, Hanna argues that we need a better understanding of "local stakeholders, power structures, and the socio-political context, to set the enabling policy reforms and institutional conditions to sustain transformation. The political orientation of the government is critical in determining the role of the state, the role of other actors, and the scope for reforms and ICT-enabled development" (Hanna 2010, p. 395, 396).

Renewable Energy and ICT in the Context of sub-Saharan Africa

As Ouedraogo et al. state "[r]enewable energy can help developing countries meet their sustainable development goals through access to clean, secure, reliable and affordable energy. The scarcity and the depletion of conventional energy resources, with rising fuel prices and harmful emissions from fossil fuels, make electricity production from conventional energy sources highly unsustainable and economically unviable" (Ouedraogo et al. 2015).

These problems of current energy access in Africa raised by Ouedraogo et al. are predominant in sub-Saharan Africa as Gujba et al. point out: "To take the case of the power sector, the installed generation capacity in the content is only about 122.6 GW, which accounts for just 2.6% of the total world installed capacity as at 2008. The electricity consumption of 571 kWh per capita is also only about five times less than the world average. Excluding Northern African countries and South Africa, installed electricity generation capacity in the rest of Africa is about

31 GW, suggesting the per capita electricity consumption in the sub-region is much lower than the African average. Compounding the problem is the alarmingly low rate of electrification in sub-Saharan Africa where only about 31% of the population has access to electricity (with 14% electrification in the rural areas), contrasting with Northern Africa which has about 99% electricity access. In addition, those connected to the grid also have to contend with highly unstable and unreliable electricity supplies, contributing to the difficulties in doing business and resulting in significant revenue losses to firms and the economy" (Gujba et al. 2012, p. 71).

At the same time the interplay of renewable energy and ICT is helping more and more people – especially in developing countries – to get connected to the modern world and profit from utilities powered by renewable energy. As McHenry and Doepel argue, there is already a revolution of low power DC energy systems and payment options under way:

> Today billions of portable information and communication technology (ICT) devices, including smartphones, tablets, lights, MP3 players, electric gardening equipment, PCs and many accessories with rechargeable batteries are now in circulation world-wide, and are increasingly associated with user energy autonomy and energy efficiency. This includes the most non-industrialised regions of the world. For example, when around 63% of people in sub-Saharan Africa have access to improved drinking water, and only around 30% have access to centralised electricity services; access to mobile phones have grown from practically zero to around 50% in only a decade. Why is this so? In contrast to the 'hard won' capital-intensive conventional electricity and water infrastructure investments by governments and international agencies, the swift adoption of ICT and the roll-out of the associated infrastructure has occurred relatively autonomously on a largely commercial basis in a very short timeframe. (McHenry and Doepel 2015, p. 679)

It is especially people living beyond the grid who are benefiting from the combination of renewable energy and ICT technology as "[t]he vast majority of rural poor populations in non-industrialised nations have no access to reliable, safe, healthy and affordable centralised electricity services. Where access does exist, economic barriers often predominate, as many rural poor households cannot afford to connect to a centralised electricity network. For these households to enjoy the benefits of modern utility services, small-scale systems must become, are becoming, a cost-effective alternative in remote areas" (Ibid., p. 679).

Gujba et al. conclude that Africa "faces huge challenges in expanding and improving access to clean and modern energy services. The potential and variety of renewable energy resources in Africa provide great opportunities for the continent to develop the energy sector at the local, national and regional levels to expand modern energy access and meet its developmental challenges in a low carbon trajectory." For the authors it is access to finance which is one of the most crucial issues that need to be addressed if Africa is to meet these objectives. They criticize that even though there are "many financial instruments and funds that Africa can take advantage of in financing low carbon energy initiatives including domestic, private, multilateral and bilateral sources," there is little investment in low carbon energy initiatives in Africa. This is in their view due "to lack of enabling policies that foster trade and investment, low levels of in-country technical skills, etc. These barriers

have left a large financing gap for low carbon energy initiatives and enterprise development in the continent" (Gujba et al. 2012, p. 77).

While there is a high mobile Internet penetration rate, incentive to use mobile Internet technologies in Africa seems to be still low. At the same time there are big opportunities in the area of low power DC utilities powered by renewable energy through mini power grids. At the same time there are international ambitions to allow for sustainable development as formulated in goal seven of the SDGs. We would like to look at the case of off-grid solar and mobile technologies in Africa to showcase this with an example.

Off-Grid Solar and Mobile Technologies

In order to better understand the potential of renewables in combination with ICT, we would like to look into the case of off-grid solar lighting and ICT. About 1.2 billion people living without access to the power grid spend about $27 billion annually on lighting and mobile-phone charging with kerosene, candles, battery torches, or other fossil-fuel powered stopgap technologies (BNEF/Lighting Global 2016, p. 2).

Off-grid solar is helping to enable access to basic electricity services. The report states that it is an estimated number of 89 million people in Africa and Asia who profit as well as 21 million individuals who were lifted to the first rung of the energy ladder. But there is no equal development of the market: "Kenya, Tanzania and Ethiopia are Africa's leading markets, accounting for 66 percent of unit sales in the region, and India is leading the way in Asia. The efforts of development institutions such as the World Bank Group and activities of social enterprises like SunnyMoney helped build these markets, and there remain many countries where the sector can expand. Simple portable lanterns that retail for less than $20, and more recently for as little as $5, have accounted for 59 percent of all pico-solar unit sales to date" (ibid; Diecker et al. 2016).

Now after a decade pico-solar is in the middle of becoming mainstream. The report finds that off-grid solar has not yet even scratched the surface of its potential globally. At the same time, it is "no longer a niche product in the countries that have seen the most concentrated sales efforts. In Kenya, more than 30 percent of people living off the grid have a solar product at home, according to the estimates of the report" (ibid.).

But there are also problems entailing the quick and successful rise of these technologies. It is especially generic products that are a problem for the market: "The market for cheap, generic pico-solar products – unbranded items or copies of branded ones – is at least as big as the brand-quality market in number of units sold and takes global sales to more than 44 million to date," according to the report. This is indeed a big challenge to the market, concludes the report, as "these products challenge the brand-name incumbents with lower prices and increase the risk of market spoilage due to unpredictable quality and a lack of warranties or after-sales service." This challenge has been answered by companies through the provision of services: "Off-grid solar brands have reacted to the rising competition by focusing

on developing distribution networks, trying to sell more powerful systems with higher margins, entering new countries or developing new applications for urban back-up lighting or camping." In addition, the report considers last-mile distribution and ongoing customer relationships as a likely value driver that will determine the successful brands (ibid.).

One strategy that is used to convince people to step over to solar off-grid solutions is to develop Pay-As-You-Go (PAYG) solutions: "PAYG firms sell solar kits against small installments instead of a lump-sum payment with a technology that locks the functionality in the event of non-payment by the consumer." This has led to big attention by investors, who put four times as much money in these solutions as in solutions based on cash payments. According to the report there are about 20 companies providing consumer financing, having almost half a million customers. These can be found manly in East Africa. Financiers pursue this strategy in the opinion of the report because "barriers to entry for new PAYG suppliers will remain higher than in the cash sale segment and that customer relationships will run deeper than in the cash sale segment and that customer relationships will run deeper" (ibid., 2, 3).

The sector saw an increase of investments having attracted $511 million of investment according to the report. PAYG companies have gotten the most attention with an investment of $160 million in 2015 alone. Interestingly, off-grid solar is advancing beyond simple lighting and phone charging solutions. By 2020 estimates are that seven million off-grid households in the developing world will use solar-powered fans and 15 million households will have a solar-powered TV. The conclusion of the report is that a company's success is related to the development of distribution networks and good customer relations (ibid., p. 3).

We now would like to take a closer look at the role that ICT and especially mobile technologies play in enabling energy access. For this purpose, we would like to look at the Mobile for Development Utilities (M4D) program of the GSM Association (GSMA 2016a). The GSMA is an association of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem. This includes handset and device makers, software companies, equipment providers, and Internet companies, as well as organizations in adjacent industry sectors. The GSMA is also responsible for industry-leading events such as the Mobile World Congress, the Mobile World Congress Shanghai, and the Mobile 360 Series conferences (GSMA 2016a, p. 2).

Through its Mobile for Development (M4D) Utilities program, GSMA aims to "promote the use of mobile technology and infrastructure to improve or increase access to basic utility services for the underserved." This program focuses on "any energy, water or sanitation services which include a mobile component such as mobile services (voice, data, SMS, USSD), mobile money, machine-to machine (M2M) communication, or leverage a mobile operator's brand, marketing or infrastructure (distribution and agent networks, tower infrastructure)." Through an own innovation fund set up with the help of the UK government, GSMA started to test and scale the use of mobile to improve or increase access to energy, water, and sanitation services. The fund was designed in two phases "of funding, grants were competitively awarded to 34 organisations across the globe. This included seed

grants for early stage trials, market validation grants for scaling or replication of business models, and Utility Partnership grants to foster partnerships between utility companies and innovators" (GSMA 2016a, p. 2).

GSMA argues that mobile channels "underpin the PAYG model in two ways." One being to "enable payment collection through mobile money or other forms of mobile payment" and the other being to "update and control PAYG-enabled assets or services through M2M or mobile services, such as SMS or mobile apps." Mobile-enabled PAYG therefore meets important needs for customers and service providers across sectors. For customers "it is affordable and convenient for those with irregular incomes." Therefore, PAYG helps to expand the addressable market significantly according to GSMA and to build "consumer trust by offering a low-risk, low commitment trial." This is seen to help regain trust, which has been damaged by low-quality solar products. The benefits for service providers through PAYG are that it "allows more efficient and secure payment collection, digital payment records, and gives customers an incentive to pay regularly since the service is suspended if they default." It is also mobile network operators (MNOs) who have both enabled and benefitted from mobile payments for PAYG services (GSMA 2016a, p. 18).

One good practice example is Fenix International, a Solar Home Systems (SHS) provider and Phase 1 grantee of GSMA's M4D utilities program. "The company was the third largest MTN Money (http://www.mtn.com.gh/personal/mobile-money/about-mobile-money) bill pay account by volume in Uganda, with 13% of Fenix's customers new to mobile money," according to GSMA. There are further examples: "In January 2016, fellow grantee and SHS provider, Mobisol, generated USD 0.58 in monthly transaction fee revenues per SHS to MTN Rwanda. SHS owners made an average of 5.1 mobile money payments every 90 days, and 20% were new to mobile money. By providing a compelling use case for mobile money, these PAYG providers are driving mobile money penetration and usage, providing key benefits for their MNO partners. Devergy, a Phase 2 grantee, proposes to integrate MNO and energy services even more closely by offering a mobile and energy bundle to Tigo customers in rural Tanzania. The results of this project will be available in the first half of 2017" (GSMA 2016a, p. 18).

The innovation fund of M4D utilities has received many more concept notes on PAYG business models for the off-grid solar energy sector. According to GSMA, "[o]ver half of the 116 energy-related Concept Notes submitted in Phase 2 of the Innovation Fund included a PAYG model." GSMA estimates are that total sales are at 650,000 with an estimated 1200 sales per day. Furthermore, annual PAYG solar unit sales are forecast to reach 13% of the off-grid solar unit market in 2020, which represents seven million units (GSMA 2016a, p. 19).

The Case of PEG Ghana

To illustrate how cooperation between the program and partners work, we would like to look at the example of Persistent Energy Ghana (PEG Ghana).

The company received a Market Validation grant in 2013 to "replicate two different Solar-as-a-Service business models and technologies from Tanzania to Ghana. PEG licensed the technology and software, and built local sales, distribution and service operations to develop their own business providing off-grid, low-income Ghanaian households with lighting, phone charging, radios and TVs" (GSMA 2016b, p. 4).

There were several lessons learned from this partnership that we want to highlight. First of all, "the over-arching insight that emerged was that licensing new technology and business models requires significant investment of time and resources from both parties through a robust agreement and partnership. Therefore, licensing carries risks for both the licensee and licensor, and the opportunity to grow the sector through licensing requires an awareness of potential challenges. As a result of the experiences gained through this grant, PEG developed a partnership with a new solar home system provider, whereby both the new supplier and PEG allocated significant resources to build strong business operations from the start" (GSMA 2016b, p. 4).

According to GSMA, there were more specific lessons related to the above mentioned. One is that "given the nascent state of the mobile-enabled energy sector, replication requires a more hands-on approach from the licensor to transfer knowledge and technical support, and build local business operations." This makes it essential that licensees ensure that their licensors see this as a part of their own growth strategy. Another point is that the business viability of micro grids highly depends on a reliable service and minimum consumption from a certain proportion of households. There are several factors that need to be taken into account (GSMA 2016b, p. 4).

Several other lessons can be considered. There is a need for strong partnerships between mobile operators and energy providers to benefit from mobile payments. Also, a commitment to invest in "increasing customer registration, training and agent networks" is important. A focused approach is of importance for investors, who in the case of PEG raised criticism on their strategy to pursue two different business models and technology at once. This led PEG to focus on solar home systems only. Clear regulation plays a crucial role for the success of business (GSMA 2016b, p. 5).

Conclusion

The example of Global Energy Governance shows the complexity of the task to enable energy access by bringing necessary knowledge/technology to where it is most needed. Going back to the argument of Carayannis et al., we have to consider the ever growing complexity of social and economic relations in the light of globally perceived problems. This makes it necessary to think further the "network-style linkage of knowledge" (Carayannis et al. 2012) with academia, government, and industry at the center not only in a self-referential way but in the shifting context of actual innovative practices that feedback into the model of the Quadruple and

Quintuple Helix Innovation Theory, by this including civil society (public-civil society-private partnerships), democracy (knowledge democracy), and social ecology. To truly be able to consider innovation in the context of environmental and ecological issues, we also need to consider how innovation can translate into concrete outputs.

Casaramona et al. show that there are many issues when taking innovation into the context of transferring knowledge/technology in the context of another country: Cultural aspects, including innovation culture, rigid administrative and regulatory framework, researchers' mobility obstacles, complex and not recognized patent exploitation procedures and IPR process, and lack of smart specialization strategies do have an enormous impact outside of bilateral cooperation as well. One might even suggest that issues multiply when put into a global context of technology transfer with all its additional complexities (see Casaramona et al. 2015, p. 505, 506).

In addition, we are dealing with not only one or two contexts of innovation but with often regional programs including a multitude of countries across continents. This ecosystem of Global Governance and in our case Global Energy Governance (GEG) is itself a very fragmented ecosystem for innovation. Political interests play a decisive role when it comes to energy governance, may it be in a North-South or South-South perspective. The case of introducing off-grid solar lighting products to the context of developing countries shows that there are many challenges from a policy perspective. Political frameworks in countries might have created dependencies and loyalties through fuel subsidies. Gaining access to renewable energy might also decrease these dependencies and allow people increased independence. Therefore, energy access has to be also seen in a way as a project of increasing personal freedoms of people.

Further challenges come with the globalized structure of energy production and technology transfer. In the case of off-grid renewable energy products, production often takes place in China, while markets can be found in Africa, India, and other places. The therefore long supply chains are a particular challenge, because of the lack of proper regulatory frameworks. Another important point is the approach in a country to appropriate regulation of existing off-grid energy markets.

From an international perspective, technology transfer and IPR play a dominant role in shaping policies that shall enable the dissemination of renewable energy technologies. But we should not forget to consider that countries always have varying goals. While some might want to favor economic development in a short time perspective, others might be more open to find a more sustainable solution for development that can also benefit from renewable energy and ICT. In accordance with key goals of Global Energy Governance (see Van de Graaf and Colgan 2016), we propose the following visualization of goals that we believe are most important to understanding energy access beyond the grid (Fig. 2).

One important factor in the context of developing countries as the example of the off-grid solar lighting sector shows is the involvement of the private sector. There is growing attention to innovative business in developing countries and big criticism of the current economic system, because it favors developed countries over developing countries. Despite the challenging business environment in developing countries,

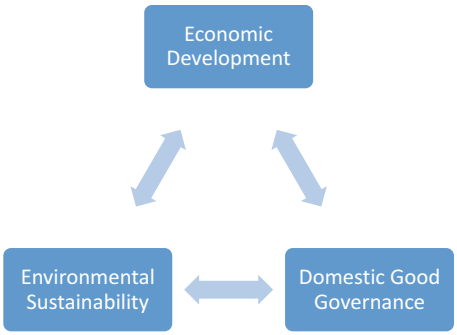


Fig. 2 Visualization of global energy governance (Source: Own conceptualization by the authors)

private sector initiatives are able to develop new and highly sustainable business models out of innovative partnerships creating multiple sources of value. But there needs to be still more understanding about the role of the private sector in partnerships aiming to achieve sustainable development (Valente 2010, pp. 49–52).

As we have seen with the example of the off-grid solar lighting sector and ICT, initiatives between the public and private sector are already aiming at changing markets in developing countries. Future research will, in this regard, need to focus on evolving sectors and public-private initiatives. This is crucial to understanding and measuring the degree to which innovative practices help in achieving universal and sustainable energy access for all by 2030.

It might be the case that we would need to broaden and develop further the concept of the Quadruple and Quintuple Helix Innovation Theory, so as to really grasp innovation on the level of global governance and how it is reinstated on the local level (Campbell 1994). As Leydesdorff puts it, there should be no limitation in the number of helices. He even argues that there could be more than 20 potential helices. But he also cautions scholars to overextend the theory and rather grow it step-by-step to gain explanatory power (Leydesdorff 2012).

The shape technology transfer is taking in a market setting of a growing knowledge economy makes it necessary to think about the interrelations spanning continents and filters that enable the scholar to better understand the connection between the receivers and providers of technology or knowledge. In Quadruple and Quintuple Helix Innovation Theory, the set-up and roles of actors and structures as well as fast paced change will be a necessary and challenging task. To achieve this, it might be necessary to draw on lessons from other approaches such as "pro-poor innovation theory" (see Berdequé 2005).

We would like to highlight that global energy challenges are an integral part for any further innovation strategy that wants to take sustainable development seriously. As the literature on global energy governance shows, there still is a lack of empirical evidence of the state of energy access and its governance. This is particularly true when considering needs, capacities, and priorities for innovation in developing countries. While there are already some studies considering bilateral or national innovation systems in developing countries, a better awareness of transnational networks would be rewarding. An understanding of technology

transfer that reflects Quadruple and Quintuple Helix innovation systems can improve our understanding of dissemination of innovation and an understanding of obstacles in the actor framework of the public, private, academic, and civil society sector. There are some questions that would need more specific answers: what are necessary and existing capacities for innovation in developing countries, which priorities are set, how can we better understand innovation in an international context of market-based technology transfer, how is technology transfer organized in the complex interplay of global problem-solving, and what are efficient approaches to technology transfer in reaching the goal of sustainable development when considering developing countries.

Meaningful scenarios for solving global energy challenges, such as energy poverty, require the capacities and a necessary access to resources for innovation and dissemination of technologies. This would depend on a strong commitment by providers of technology (private, public, academic, and civil society) and a better understanding of needs in receiving countries in building capacities for energy access. *Furthermore, this implies to agree on a multidimensional commitment not only including knowledge or technology transfer, but assistance with shaping a sustainable environment for energy access, including academic, entrepreneurial, and vocational capacities. In the end, successful dissemination of innovation is of mutual interest on a global scale, since results can make a difference in an ecological, social, and economic perspective*.

References

Abdel-Latif, A. (2015). Intellectual property rights and the transfer of climate change technologies: Issues, challenges, and way forward. *Climate Policy, 15*(1), 103–126.

Andrade, J. C. S., & de Oliveira, J. A. P. (2015). The role of the private sector in global climate and energy governance. *Journal of Business Ethics, 130*, 375–387. https://doi.org/10.1007/s10551-014-2235-3.

Berdequé, J. A. (2005). Pro-poor innovation systems. Background paper. Rome: IFAD.

Biermann, F., Pattberg, P., van Asselt, H., & Zelli, F. (2009). The fragmentation of global governance architectures: A framework for analyis. *Global Environmental Politics, 9*(4), 14–40.

BNEF/Lighting Global. (2016). Off-grid solar market trends report 2016.

Brandenburger, A. M., & Nalebuff, B. J. (1997). *Co-opetition*. New York: Doubleday.

Bush, V. (1945*). Science: The endless frontier*. Washington, DC: United States Government Printing Office. http://www.nsf.gov/od/lpa/nsf50/vbush1945.htm#transmittal

Campbell, D. F. J. (1994). European nation-state under pressure: National fragmentation or the evolution of suprastate structures? *Cybernetics and Systems: An International Journal 25*(6), 879–909. http://www.informaworld.com/smpp/title~db=all~content=g770888219

Campbell, D. F. J., & Carayannis, E. G. (2012). Lineare und nicht-lineare knowledge production: Innovative Herausforderungen für das Hochschulsystem. *Zeitschrift für Hochschulentwicklung 7*(2), 64–72. http://www.zfhe.at/index.php/zfhe/article/view/448

Campbell, D. F. J., & Carayannis, E. G. (2013a). *Epistemic governance in higher education. Quality enhancement of universities for development* (SpringerBriefs in Business). New York: Springer. http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6

Campbell, D. F. J., & Carayannis, E. G. (2013b). Epistemic governance and epistemic innovation policy, 697–702. In Carayannis, E. G. (Editor-in-Chief), Dubina, I. N., Seel, N., Campbell D. F. J., Uzunidis, D. (Associate Editors), *Encyclopedia of creativity, invention,*

innovation and entrepreneurship. New York: Springer. http://link.springer.com/referenceworkentry/10.1007/978-1-4614-3858-8_271

Campbell, D. F. J., & Carayannis, E. G. (2016). Epistemic governance and epistemic innovation policy. *Technology, Innovation and Education 2*(2), 1–15. http://technology-innovation-education.springeropen.com/articles/10.1186/s40660-016-0008-2

Campbell, D. F. J., Carayannis E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy 6*(3), 467–493. http://link.springer.com/article/10.1007/s13132-015-0246-7

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "Quadruple Helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management 46*(3/4), 201–234. http://www.inderscience.com/info/inarticletoc.php?jcode=ijtm&year=2009&vol=46&issue=3/4, http://www.inderscience.com/info/inarticle.php?artid=23374

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development 1*(1), 41–69. http://www.igi-global.com/article/triple-helix-quadruple-helix-quintuple/41959

Carayannis, E.G., & Kaloudis, A. J. (2010). A time for action and a time to lead: democratic capitalism and a new "New Deal" for the US and the world in the Twenty-first century. *Journal of the Knowledge Economy 1*: 4. https://doi.org/10.1007/s13132-009-0002-y.

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development* (SpringerBriefs in Business). New York: Springer. http://www.springer.com/de/book/9781461420613

Carayannis, E. G., & Campbell, D. F. J. (2017). The Quadruple Helix innovation systems conceptual framework, 1–7. In De Oliveira Monteiro, S. P., Carayannis E. G. (Eds.), *The quadruple innovation helix nexus. A smart growth model, quantitative empirical validation and operationalization for OECD countries*. New York: Palgrave Macmillan. https://link.springer.com/chapter/10.1057/978-1-137-55577-9_1

Carayannis, E. G., Barth, T. D., & Campbell D. F. J. (2012). The Quintuple Helix innovation model: Global warming as a challenge and driver for innovation. *Journal of Innovation and Entrepreneurship*, *1*(1), 1–12. https://innovation-entrepreneurship.springeropen.com/articles/10.1186/2192-5372-1-2

Carayannis, E. G., & Campbell, D. F. J. (2014). Developed democracies versus emerging autocracies: arts, democracy, and innovation in quadruple helix innovation systems. *Journal of Innovation and Entrepreneurship 3* (12), 1–23. http://www.innovation-entrepreneurship.com/content/3/1/12

Casaramona, A., Sapia, A., & Soraci, A. (2015). How TOI and the quadruple and quintuple helix innovation system can support the development of a new model of international cooperation. *Journal of Knowledge Economy, 6*, 505–521.

Danilda, I., Lindberg, M., & Torstensson, B-M. (2009). Women resource centres: A quattro helix innovation system on the European agenda, Paper. http://www.hss09.se/own_documents/Papers/3-11%20-%20Danilda%20Lindberg%20&%20Torstensson%20-%20paper.pdf

De Coninck, H., & Puig, D. (2014). Assessing climate change mitigation technology interventions by international institutions. *Climatic Change, 131*(3), 417–433.

Diecker, J., Wheeldon, S., & Scott, A. (2016): Accelerating access to electricity in Africa with off-grid solar: Policies to expand the market for solar household solutions, Report. Overseas Development Institute (ODI). https://www.odi.org/publications/10200-accelerating-access-electricity-africa-off-grid-solar

Dubash, N. K., & Florini, A. (2011). Mapping global energy governance. *Global Policy, 2*(special issue), 6–18.

Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation: From national systems and "mode 2" to a triple helix of university-industry-government relations. *Research Policy, 29*, 109–123.

European Commission. (2009). *The world in 2025: Rising Asia and socio-ecological transition*. Brussels: European Commission. http://ec.europa.eu/research/social-sciences/pdf/the-world-in-2025-report_en.pdf

Fischer-Kowalski, M, Haberl, H. (Eds.) (2007). *Socioecological transitions and global change. Trajectories of social metabolism and land use*. Cheltenham: Edward Elgar.

Florini, A., & Dubash, N. K. (2011). Introduction to the special issue: Governing energy in a fragmented world. *Global Policy, 2*(special issue), 1–5.

Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P., & Trow, M. (1994). *The new production of knowledge. The dynamics of science and research in contemporary societies*. London: Sage.

Goldthau, A. (Ed.). (2013). *The handbook of global energy policy.* West Sussex: John Wiley & Sons.

GSMA. (2016a). Unlocking access to utility services: The transformational value of mobile. Mobile for development utilities annual report. http://www.gsma.com/mobilefordevelopment/programmes/m4dutilities/annual-report

GSMA. (2016b). *Mobile for development utilities*. PEG Ghana: Licensing Solar-as-a-Service in a New Market. http://www.gsma.com/mobilefordevelopment/programme/m4dutilities/peg-ghana-licensing-solar-as-a-service-in-a-new-market

Gujba, H., Thorne, S., Mulugetta, Y., Rai, K., & Youba, S. (2012). Financing low carbon energy access in Africa. *Energy Policy, 47*(2012), 71–78.

Hanna, N. K. (2010). *E-transformation: Enabling new development strategies*. New York: Springer.

Hardin, G. (1968). The tragedy of the commons. *Science, 162*, 1243–1248.

Haselip, J., Elmer Hansen, U., Puig, D., Trærup, S., & Subash, D. (2015). Governance, enabling frameworks and policies for the transfer and diffusion of low carbon and climate adaptation technologies in developing countries. *Climatic Change, 131*(3), 363–370. https://doi.org/10.1007/s10584-015-1440-0.

Hemlin, S., Allwood, C. M., & Martin, B. R. (2004). *Creative knowledge environments. The influences on creativity in research and innovation*. Cheltenham: Edward Elgar.

IEA. (2012). *World energy outlook 2012*. OECD/IEA. Paris.

Internet Society (2016). *Global Internet Report 2015: Mobile evolution and development of the internet*. http://www.internetsociety.org/globalinternetreport/#main-content

Lakamp, B (2017). Energy is the new Internet. Crunch Network. https://techcrunch.com/2017/01/22/energy-is-the-new-new-internet/?ncid=rss&utm_s

Leydesdorff, L. (2012). The triple helix, quadruple helix, and an N-tuple of helices: Explanatory models for analyzing the knowledge-based economy? *Journal of the Knowledge Economy 3*(1), 25–35. http://link.springer.com/article/10.1007/s13132-011-0049-4

McHenry, M. P., & Doepel, D. (2015). The “low power” revolution: Rural off-grid consumer technologies and portable micropower systems in non-industrialised regions. *Renewable Energy, 78*(2015), 679–684.

De Oliveira Monteiro, S. P., & Carayannis E. G. (2017). *The quadruple innovation helix nexus: A smart growth model, quantitative empirical validation and operationalization for OECD countries*. New York: Palgrave Macmillan. http://www.palgrave.com/br/book/9781137555762

Nowotny, H., Scott, P., & Gibbons, M. (2001). *Re-thinking science. Knowledge and the public in an age of uncertainty.* Cambridge, UK: Polity Press.

Nowotny, H., Scott, P., & Gibbons, M. (2003). Mode 2 revisited: The new production of knowledge. *Minerva, 41*, 179–194.

Nowotny, H., Scott, P., & Gibbons, M. (2006). Re-thinking science: Mode 2 in societal context, 39–51. In E. G. Carayannis & D. F. J. Campbell (Eds.), *Knowledge creation, diffusion, and use in innovation networks and knowledge clusters. A comparative systems approach across the United States, Europe and Asia*. Westport: Praeger.

Oueraogo, B. I., Kouame, S., Azoumah, Y., & Yamegueu, D. (2015). Incentives for rural off grid electrification in Burkina Faso using LCOE. *Renewable Energy, 78*(2015), 573–582.

Pattberg, P., & Widerberg, O. (2014). Theorising global environmental governance: Key findings and future questions. *Millenium, 43*(2), 684–705.

Pattberg, P., & Widerberg, O. (2016). Transnational multistakeholder partnerships for sustainable development: Conditions for success. *Ambio, 2016*(45), 42–51.

Polanyi, M. (1962). The republic of science: Its political and economic theory. *Minerva 1*, 54–74. http://sciencepolicy.colorado.edu/students/envs_5100/polanyi_1967.pdf, http://fiesta.bren.ucsb.edu/~gsd/595e/docs/41.%20Polanyi_Republic_of_Science.pdf

Pueyo, A. & Linares, P. (2012). Renewable technology transfer to developing countries: One size does not fit all. IDS working paper 412. http://www.ids.ac.uk/publication/renewable-technology-transfer-to-developing-countries-one-size-does-not-fit-all

Rosenau, J. N. (1997). Along the domestic-foreign frontier: exploring governance in a turbulent world, Cambridge Univ. Press, Cambridge.

SE4ALL. (2014). 2014 annual report. http://www.se4all.org/content/se4all-2014-annual-report

Shugurova, I. V. & Shugurov, M. V. (2015). International technology transfer – Controversial global policy issues. *Environmental Policy and Law, 45*(3), 133–139.

Stamm, A., Figueroa, A., & Scordato, L. (2012). Addressing global challenges through collaboration in science, technology and innovation. In *OECD, meeting global challenges through better governance: International co-operation in science technology and innovation*. Paris: OECD Publishing.

UN. (2015). General Assembly Resolution 70/1, Transforming our world: The 2030 Agenda for Sustainable Development, A/RES/70/1 (21 October 2015). Available from Paris http://undocs.org/A/RES/70/1

Valente, M. (2010). Public and private partnerships for sustainable development in Africa: A process framework. *Journal of African Business, 11*(1), 49–69. https://doi.org/10.1080/15228911003608538.

Van de Graaf, T. & Colgan, J. (2016). Global energy governance: A review and research agenda. Palgrave Communications 2, Article number: 15047 (2016). http://www.palgrave-journals.com/articles/palcomms201547

Digitalization of Tax: Epistemic Tax Policy

6

David F. J. Campbell and Georg Hanschitz

Contents

Abstract

Digitalization, automatization, and social media interaction do not only influence our everyday lives but also change the way we think (Naughton, J. The internet: Is it changing the way we think? *The Guardian*, 2010) and especially, how we solve complex tasks. People search and find answers to complex questions via Google,

D. F. J. Campbell (✉)
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@univie.ac.at; david.campbell@uni-ak.ac.at; david.campbell@aau.at

G. Hanschitz
Institute of Education and Innovation, Vienna, Austria
e-mail: mail@georghanschitz.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_30

Apple Siri, Amazon Echo, and all different types of expert-platforms. The more complex the questions are, the more often online-based answers are searched, and it seems to work in a lot of cases: in 2011, "IBM's Watson question-answering system won the TV gameshow Jeopardy" (Jurafsky and Martin 2017). This analysis is about a special sort of jeopardy. It is about one of the most dominant topics for entrepreneurs and self-employed people: the tax system. In the following, the complexity of tax regimes will be discussed within the frame of its digitization ability and with a modern interpretation of the concept of disruption, an economic concept by twentieth-century economist Josef A. Schumpeter (Pyka and Andersen 2013): What can be digitized will be digitized – sooner or later. By analyzing digital tax administration, this analysis is an academic contribution to the ongoing debate of digital facilitation versus digital disruption, how far digital applications should be used to make old systems just more efficient or can only be efficient, if used to design new disruptive digital systems. In near future, digital end-to-end tax systems might replace today's complex preregistration tax regimes for entrepreneurs and self-employed people. Online tax accounts eliminate the problem of "unreported income" and can make the tax declaration of individuals (employees or self-employed) and of companies (particularly of small-sized and medium-sized enterprises) much easier and cheaper, because then public tax authorities also would provide new services and service qualities. In addition, there is a need for an Epistemic Tax Policy, which offers opportunities to see, whether the designed and applied tools in taxation meet the test of reality; this furthermore leads to routes of further improving tax systems.

Keywords
Blockchain · Cash register · Corporate tax · Digitalization · Digitalization of tax · Online tax accounts · Epistemic Tax Policy

Introduction

This analysis is a contribution to the discussion on how cyber-development and digitalization will change the way how public administrations deal with their residents. Citizenship and monetary participation are linked since the third millennium BC. Documents of that time show that in Egypt administrators called for a harvest tax and a Nile-tax (Klinkott et al. 2007). Today, federal and local budgets are still tax based. But over the time, tax systems and regimes became more and more complicated. It has gotten so complex that there is a ranking of the "easiest and most complex jurisdictions in the world for accounting and tax compliance". The "Financial Complexity Index 2017" (The Financial Complexity Index 2017), published by the "Netherlands-headquartered TMF Group," examines "the varied complexities of maintaining accounting and tax compliance across 94 jurisdictions worldwide." But with new digital structures and mobile applications, there are new possibilities to raise tax-income without raising taxes.

Digitalization of Tax Regimes: The Macroeconomic Dimension

A study of the University of Chicago showed that in 2012 Greek self-employed workers and freelancers hid almost half of their income in front of the financial authorities in 2009. According to the study, the deducted taxes amounted to 11.2 billion euros. If freelancers and self-employed honestly pay their taxes, the country would be far better off, the study concludes (The Financial Complexity Index 2017).

Tax fairness has a lot of dimensions, but it is a macroeconomic truth that when everyone pays taxes, everyone pays less taxes (Smith 1776; Wagner 1880; Neumark 1970). For that reason, the IMF started to consider the implementation of electronic devices in different developed states and evaluated the results (IMF, WP/15/73).

After several administrations implemented electronic fiscal devices (EFDs) in their tax system for sales and value-added tax (VAT), the IMF concluded that it hakes "effort and has costs both for the administration and for the taxpayers that are affected by the requirements" and "despite their widespread use, and their considerable cost, EFDs can only be effective if they are a part of a comprehensive compliance improvement strategy that clearly identifies risks for the different segments of taxpayers and envisages measures to mitigate these risks" (Casey and Castro 2015).

The IMF summed up EFDs "as with any other technological improvement the deployment of fiscal devices alone cannot achieve meaningful results, whether in terms of revenue gains or permanent compliance improvements" (Casey and Castro 2015).

After considering these experiences by the IMF, one can say that EFD implementation would be more effective with the use of an online tax account system communicating with mentioned fiscal devices. EFDs, like electronic tax registers, are more effective when they are not stand-alone-units but work together with fiscal data applications of governments (tax administrations). Information exchanges between tax administrations and companies lead to better tax transparency, easier tax collection, and tax fairness.

Digital Facilitation Versus Digital Disruption

Today, especially tax consultants are responsible for tax transparency. In many cases, they are the link between the tax administration and tax payers, particularly when they are companies or self-employed people. But tax consultants may face the end of their business basis when tax administrations start to implement digital tax systems to generate more information, payment, and legal security. From the time when the process of digitalization started in the 1990s, traditional tax consultants have tried to implement more online services in their customer relations business. But the question is, if this will be enough to compete with the possibility to a digitalized tax administration in future.

Digital Facilitation

Germany is one of the top-rated countries when it comes to tax consulting. Tax consulters state that a large share of the whole worldwide literature that is being published on tax is actually being published in the German language. But since digitization has advanced, German tax consultants face huge competition with digital tax consulting platforms, where clients get and receive personalized tax advice via the Internet. "Data and evaluations are exchanged via the secure entrepreneurial portal, the accounting is done in the cloud" (felix1.de AG 2017). Traditional German tax consultants are not used to face any sort of business-threatening competition. What happened in Germany some years ago, in the field of tax consulting, was some type of transformation of service: from human interaction to digital facilitation. Online tax consultants for companies, entrepreneurs, and private individuals facilitate tax management via online collection of data (incomes, revenues, expenses, salaries) by OCR-scanning (optical character recognition) applications or input by hand. Since online-tax-applications gained market shares, traditional tax consultants have to deal with the change of their business and try to develop new business areas for themselves using client consulting software (dpa in Handelsblatt 2016). It is pretty clear that all potentials of facilitation of online tax that consultants use today, could also be used by federal tax administrations, so:

- What if governments and tax administrations begin to digitalize their tax regimes?
- Is a future thinkable where individuals and small-company owners have the possibility to interact with tax administrations like with banking houses: having an always-on account?

Estonia already integrated digital signatures and electronic tax claims that have already lowered bureaucracy and facilitated tax management. "In Estonia 98% of companies are established online, 99% of banking transactions are made online and 95% of tax declarations are filed online" (e-estonia 2017). But Estonia is not the only country in Europe, changing the way of generating tax.

In the UK, the government's plan "to make it easier for individuals and businesses to get their tax right and keep on top of their affairs" is called "Making Tax Digital." The UKs "Making Tax Digital roadmap" was published in December 2015 and will be implemented completely in 2020. "By 2020, customers will be able to see a comprehensive financial picture in their digital account, just like they can with online banking" (UK Government 2017).

Since 2016, in Austria, taxable businesses are required to issue receipts via electronic cash registers to all customers for payments made in cash, by bank cards, credit cards, or debit cards and also electronic payments (paypal, mobile phone). All payments that are being made are registered by an electronic recording system in the cash register. This cash register requirement is mandatory for businesses with a minimum net annual revenue of 15,000 Euro or if annual cash transactions exceed 7500 Euro. The register collects data in a data collection log and since April 1, 2017, electronic cash registers have to have an electronic signature to be protected against any kind of manipulation.

Every receipt has a signature with a machine-readable code (in the form of a QR code), which is attributable to a certain data-record in the machine. So, as a consequence, all incoming payments can be followed by the tax administration.

It is likely that cash register obligations were only a first step in a direction of business (VAT) and corporate tax administration. The electronic cash register has been designed as an instrument for verifiability sales; the state has created an opportunity to examine the taxed turnover of companies with the help of IT systems. At the moment, the use of the registration system by the state ends with the verifiability of sales. But there are more possibilities by implementing digital end-to-end systems in tax regimes.

Digital Disruption

With the possibility of internet connected cash registers, sending information about turnover and sale volumes directly to the federal tax office, it would also be possible to deduct tax instantly after a business deal from an online tax account. Corporate tax obligations could be deducted automatically from a corporate tax account.

In 2012, the Austrian government started to automatically deduct taxes of stock exchange gains administrated by stock market platforms and banks that have a mandate and obligation to send volume, buyer, and seller information directly to the federal tax office (BMF 2017). The gain tax coming from stock exchange business is directly deducted from the account of the business practitioner who gains capital in the selling process. The result: full payment of tax obligations and legal security.

In other business activities, the tax prepayment is used to tax corporations (Casapicola 2016) which means that depending on revenue, managers and owners are obliged to send monthly or quarterly forecasts and tax payments to the federal tax office, including all problems concerting business volatility.

By linking the electronic accounting systems of companies (including all cash registers) with the online accounts that the companies have with the tax administrations, all tax obligations resulting from turnover could be received directly. The accounting system also includes tax-deductible items like fixed costs, social insurance, or payments to employees in the overall tax evaluation. Like a second bank account, with incoming and outgoing obligations, the tax-application becomes an integrated part of the daily accounting business.

Small- and medium-sized companies in particular would benefit from digitization, as they frequently do not have in-house tax experts, and furthermore, for self-employed persons, the implementation of such a digitalized turnover system would be a huge advantage: a virtual account that bundles all revenue, payments to social security system and pension funds. Economically, a direct link between turnover and tax via electronic applications would mean a reduction of current administrative tasks of companies and self-employed persons, particularly in the calculation of income taxes for small- and medium-sized enterprises.

An online tax account for the self-employed would also reduce bureaucratic hurdles of self-employment. The importance of taxes in entrepreneurial decisions

were also part of academic studies: "An irrational strong importance of taxes in an individual's decision-making behavior is one of the most popular assumptions about the behavioral effects of taxation" (Hundsdoerfer and Sichtmann 2008). In 2008, a study about the importance of taxes in entrepreneurial decisions showed that "tax aspects are over weighted in entrepreneurial decision-making" (Hundsdoerfer and Sichtmann 2008). A reduction of administrative tasks like tax accounting would also influence entrepreneurial decisions in a positive way.

The Development of Online Tax Accounts and Just-In-Time Taxation

How far are we away from digital "just-in-time taxation"? Tax administrations around the world are developing theirs regimes faster than companies may think.

Finland has created an income register that should be introduced at the end of 2018: The description of the project by the Finnish Tax Administration was, in May 2017, as is: "From 1 January 2019, the information contained in the Incomes Register will be used by the Tax Administration, the Social Insurance Institution (Kela), the Unemployment Insurance Fund and earnings-related pension providers. From 2020, the register will also be used by the Ministry of Economic Affairs and Employment's administrative branch, Statistics Finland, the Education Fund, non-life insurance providers, unemployment funds and the Occupational Safety and Health Administration. Information can be submitted to the Incomes Register through software interface, user interface or, on special grounds, on paper" (Vero.fi 2017).

All Finnish people will get a personal user account for taking care of taxes and receive updates on a monthly basis. The idea is that companies send "tax details directly from their accounting software without any manual labour" (Kotilainen 2015).

As described before, also Estonia (E-Estonia 2017) experiences already an advanced digital tax administration: "There is a central shared platform for all government agencies and large banks; data on taxable events is collected from employers and other third parties; and citizen identification is secure and robust, enabling the Estonian Tax and Customs Board to provide pre-populated tax returns, which take just minutes to approve and submit with a digital signature. However, there is some digital exclusion among older citizens and in remote areas with poor internet connectivity" (Meall 2017).

Tax digitalization in Brazil: Brazil's tax transparency already reached a level "that the ongoing need to file annual indirect or direct tax returns may soon be redundant, or at the very least turn into simple reconciliation events" (Kielstra 2015). How did that happen? For tax transparency reasons, Brazil has imposed two main changes in its tax regime:

– "First, all billing for goods and services must now take place through one of several electronic processes. Each of these involves, as an early step, communication of the invoice to the government. Tax authorities must evaluate and approve the information on it before the transaction it covers can proceed. In effect, the authorities now know of every sale before it is legally completed and can block ones where they dispute the level of indirect tax" (Kielstra 2015).
– "Second, Brazil now requires companies to use a standardized public digital bookkeeping system (SPED) with separate subsystems for accounting and tax. These replace traditional bookkeeping ledgers and, at the end of each year, companies must submit their complete SPED files – a detailed record of every single business transaction – to the authorities" (Kielstra 2015).

Brazil's development attracted attention and so another American state initiated electronic audits; Mexico's tax authority is considered to be at the forefront of "digitizing and automating taxation" by launching electronic audits based on information filed electronically by taxpayers: "All correspondence will be conducted electronically through taxpayers' registered email accounts, and documents will be made available to taxpayers in an electronic drop-box" (Mingram and Grosselin 2016).

Just-in-time taxation: "Global taxation is moving to a just-in-time environment." (Mingram and Grosselin 2016). And as another Ernst & Young tax digitalization study shows, Brazil and Mexico are not the only countries digitalizing their tax regimes (EY Center for Tax Policy. EYG no. YY3818. 2016).

Data Security: The Most Critical Aspect of Tax Digitalization

On-time-tax-data may be one of the most confidential data of individuals, corporations, and organizations that Governments will (may) have in near future. Data leaks then could easily be used by hackers, industrial espionage, and stock exchange speculation. Therefore, consulting companies around the world develop big data solutions that provide the security needed for public just-in-time applications.

In February 2017, the consulting corporation McKinsey & Company (2017) exhibited a possible solution for the risk of unauthorized access and data manipulation by "using blockchain to improve data management in the public sector" (see Box 1). In their model, "each person or organization would have all relevant data stored in a dedicated ledger within an encrypted blockchain database" (Cheng et al. 2017). Government tax enforcement via blockchain technology is even one of the top-rated blockchain application scenarios that the consulting company Ernst & Young reported in 2016 for the next years. The main reason for this assessment is the level of security that blockchain provides.

Box 1 Options of blockchain technology for quality network services and data control for and by citizens
Image and image source: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Using%20blockchain%20to%20improve%20data%20management%20in%20the%20public%20sector/SVGZ-Using-blockchain-to-improve-ex1.ashx
Source: McKinsey & Company 2017

Ernst & Young explains the security of blockchain because of their nature being "distributed databases containing records of every transaction ever made among participants in a given network, encrypted into time-stamped blocks via a cryptographic hash function. Each block's hash result is a unique identifier and is incorporated into the next block for integrity verification. Blockchains further protect data integrity by distributing a full copy of the database to each participant; revisions must be agreed to by a majority of participants. Blockchain's hash function plus its majority consensus approach add up to a powerful new approach to information security" (Flynn 2016).

Another consulting company providing blockchain security models for governments and public administrations is IBM. On January 11, 2017, IBM Watson Health announced a collaboration with the US Food and Drug Administration (FDA) to study the "Use of Blockchain Technology for Secure Exchange of Healthcare Data" (IBM Watson Health 2017). And on July 29, 2017, the Chinese electronic taxation enterprise "Miaocai Network" announced on its official website that it develops a "tax electronic invoice system and social tax-collecting service" for China: "The Chinese government will utilize blockchain technology for social taxation and electronic invoice issuance matters" (Du 2017). From an analytical standpoint, it appears likely that blockchain technology will be the enabler or potential enabler of public just-in-time applications worldwide.

Outlook

Cyber-development and digitalization will lead to just-in-time services of public administrations. By implementing online services, the tax administration will lose complexity and new digital applications will make it easier to handle tax accounts and *to raise tax-income without raising taxes*. As different countries digitalize their tax regimes, one of the biggest issues is data security. With the implementation of blockchain technology in public administration services, it appears likely (or at least possible) that one of the biggest hurdles for implementing just-in-time tax administration can be solved in the near (or next) future.

In the following, the analysis on the digitalization of tax and taxes should be complemented by referring finally to the following issues and challenges. This opens up perspectives for further discussion opportunities:

1. **Online tax accounts for employment-based and self-employment-based incomes of individuals (individual income tax returns)**: The creation of online tax accounts by (and for) individuals (self-employed or also employed in a standard setting) implies that tax authorities know about these incomes and that because of this, this is a declared income and by definition no "black money." Based on the flows through these online tax accounts, tax authorities either automatically could create taxes or report possible taxes but should also inform the individuals (or tax payers) about options of tax deductions (for now or later). Tax authorities also could automatically repay a possible overpay in tax. *The advantage here is that individuals do not have to consult expensive tax consultants and do not have the risk to have "unreported income."* Taxation (and reporting) of self-employed income then would also not be more complicated than the taxation of employment-based income.
2. **Online tax accounts in support of small businesses**: Should companies (here particularly the small- and medium-sized enterprises) create such online tax accounts, for example, for their employees, this also may imply that administrative work is taken from these enterprises, because the public tax administrations are then in a position to provide such services. The risk of failure in reporting then also would be with state (the public) and not with the (private) enterprises.
3. **Online tax accounts to be taught about at schools**: The installment and use of such online tax accounts (by and for individuals, but also for companies) could be part of the public school curriculum, meaning that pupils (as future mature citizens) are receiving here information and training of practical relevance for their lives.
4. **Companies should pay taxes based on "where" the revenues are being (have been) created**: One current problem in tax systems is the different taxation treatment of individuals in comparison with the tax options of the bigger companies (corporations). Individuals must pay taxes on the basis of their actual residence and/or location of their work place. What matters here is the real residence and real location of the work place. Corporations can create "tax headquarters" in selected countries or regions, based on specific tax incentives, meaning to finally set up headquarters there, where the tax shares are lowest. This may lead to completely artificial constructions. This also puts tax systems under comparative pressure and has led to situations of creating complex corporate structures for the purpose of minimizing the payment of taxes by exactly these corporations. Therefore, the one crucial argument here is *that companies should pay their taxes there, where the revenues actually have been created*. Digital tax regimes can provide tools for more precisely identifying and locating the "location of revenue."
5. **The possible use of tax reporting for developing statistics on the funding and funding trends of research and innovation**: It would be interesting, if public authorities would use (anonymized) information on taxes and tax revenues for creating new statistics. For example, information on research-related tax deductions could serve as an input for estimating aggregated expenditure on research (R&D) that is being generated by a multitude of companies and the business

enterprise sector as a whole. Perhaps also tax-based statistics on innovation activities would be possible.

6. **Epistemic tax policy**: The further evolution of tax regimes always is being challenged by new trends and further developments. As one possibility, unconventional types of companies may emerge, for example "academic firms" (Campbell and Carayannis 2016a). Furthermore, global tax regimes are also arising. So how can the taxation of individuals or of companies be made easier that live or that operate in different countries (more than one country) at the same time? *Therefore, tax regimes and tax policy should also be "epistemically" sensitive, in the sense that there must be a continuous reflection about the validity and reliability of the designed and applied tools in taxation: Do they fit reality and what are options for improvement* (Campbell and Carayannis 2016b)? Epistemic Tax Policy moves here forward in a strategic sense and clearly offers crucial opportunities.

Cross-References

- ▶ Academic Firm in Cyber-Development: The New Design and Redesign Proposition for Entrepreneurship in the Innovation-Driven Knowledge Economy
- ▶ Epistemic Governance and Epistemic Innovation Policy in Higher Education for Cyber-Development
- ▶ Quadruple and Quintuple Helix Innovation Systems and Mode 3 Knowledge Production

References

BMF. (2017). Bundesministerium für Finanzen. https://www.bmf.gv.at/steuern/Substanzgewinne-bzw-Einkuenfte-aus-realisierten-Wertsteiger.html. Accessed 1 July 2017.

Campbell, D. F. J., & Carayannis, E. G. (2016a). The academic firm: A new design and redesign proposition for entrepreneurship in innovation-driven knowledge economy. *Journal of Innovation and Entrepreneurship, 5*(12), 1–10. https://doi.org/10.1186/s13731-016-0040-1. http://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-016-0040-1.

Campbell, D. F. J., & Carayannis, E. G. (2016b). Epistemic governance and epistemic innovation policy. *Technology, Innovation and Education, 2*(2), 1–15. https://doi.org/10.1186/s40660-016-0008-2. http://technology-innovation-education.springeropen.com/articles/10.1186/s40660-016-0008-2.

Casapicola, G. (2016). Casapicola & Gross Wirtschaftsprüfungs- und Steuerberatungs GmbH, Wien. http://www.taxes.at/en/the-austrian-tax-system/. Accessed 1 July 2017.

Casey, P., & Castro, P. (2015). Electronic fiscal devices (EFDs). An empirical study of their impact on taxpayer compliance and administrative efficiency by Peter Casey and Patricio Castro, International Monetary Fund (IMF) WP/15/73.

Cheng, S., Daub, M., Domeyer, A., Lundqvist, M. (2017). Using blockchain to improve data management in the public sector. http://www.mckinsey.com/business-functions/digital-

mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector. Online since February 2017. Accessed 12 July 2017.

dpa in Handelsblatt. (2016). Steuererklärung in Estland. Ein Blick, ein Klick – fertig. dpa Deutsche Presse-Agentur GmbH / Nachrichtenagentur. 16.04.2016 12:10 Uhr. http://www.handelsblatt.com/finanzen/steuern-recht/steuern/steuererklaerung-in-estland-ein-blick-ein-klick-fertig/13456972-all.html. Accessed 21 Apr 2017.

Du, J. (2017). Press release, http://www.miaocaiwang.com/?do=article&id=2897 reported by http://www.coinfox.info/novosti/7335-blockchain-will-be-used-by-chinese-government-for-taxation-and-electronic-invoices-issuance. Accessed 12 July 2017.

E-Estonia. (2017). Online platform by the Estonian Government. https://e-estonia.com/solutions/business-and-finance/e-tax. Accessed 18 July 2017.

EY Center for Tax Policy. (2016). Tax administration is going digital: Understanding the challenges, EYG no. YY3818, 2016 Ernst & Young LLP. http://www.ey.com/Publication/vwLUAssets/EY-tax-administration-is-going-digital/$FILE/EY-tax-administration-is-going-digital.pdf. Accessed 12 July 2017.

felix1.de AG. (2017). Press release. https://www.felix1.de/presse/pressemitteilungen/digitale-revolution-in-der-steuerberatung. felix1.de AG Steuerberatungsgesellschaft, Berlin. Accessed 5 Aug 2017.

Flynn, C. (2016). Blockchain reaction. Tech companies plan for critical mass. EYG no: 01395–164GBL. http://www.ey.com/Publication/vwLUAssets/ey-blockchain-reaction-tech-companies-plan-for-critical-mass/$FILE/ey-blockchain-reaction.pdf. Accessed 12 July 2017.

Hundsdoerfer, J., & Sichtmann, C. (2008). The importance of taxes in entrepreneurial decisions: An analysis of practicing physicians' behaviour. *Review of Managerial Science*, *3*(1), 19–40. https://link.springer.com/article/10.1007/s11846-008-0023-0. First online: 31 Dec 2008. Accessed 12 July 2017.

IBM Watson Health. (2017). Press release Jan 11, 2017, 08:00 ET http://www.prnewswire.com/news-releases/ibm-watson-health-announces-collaboration-to-study-the-use-of-blockchain-technology-for-secure-exchange-of-healthcare-data-300389160.html. Accessed 12 July 2017.

Jurafsky, D., & Martin, J. H. (2017). Speech and language processing. https://web.stanford.edu/~jurafsky/slp3/28.pdf. Accessed 8 Aug 2017.

Kielstra, P. (2015). Business unusual: The future is here and some tax authorities got here first. EY – Tax insights for business leaders №14, EYGS LLP, on behalf of EY Global Tax, November 2015.

Klinkott, H., Kubisch, S., Müller-Wollermann, R. (2007). Geschenke und Steuern, Zölle und Tribute: Antike Abgabenformen in Anspruch und Wirklichkeit. BRILL, ISBN 9047422953, 9789047422952.

Kotilainen, S. (2015). Interview with Pekka Ruuhonen, Director General of the Tax Administration, in Net Magazine 1/2015. http://www.net.fujitsu.fi/en-US/12015/The_Tax_Administration_going_electronic_(7678). Accessed 10 July 2017.

McKinsey & Company. (2017). Picture URL: http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Using%20blockchain%20to%20improve%20data%20management%20in%20the%20public%20sector/SVGZ-Using-blockchain-to-improve-ex1.ashx. Accessed 12 July 2017.

Meall, L. (2017). Digital tax administration is here. AB magazine. http://www.accaglobal.com/uk/en/member/member/accounting-business/2017/04/practice/digital-tax.html. Accessed 10 July 2017.

Mingram, A., & Grosselin, T. (2016). At the intersection of international tax and digital transformation. Just-in-time taxation. Content first published in Global Tax Weekly 24 November 2016. Online http://www.ey.com/Publication/vwLUAssets/EY_GTW_Just_in_time_taxation_Final/$FILE/EY_GTW_Just_in_time_taxation_Final.pdf. Accessed 12 July 2017.

Naughton, J. (2010). The internet: Is it changing the way we think? The Guardian. https://www.theguardian.com/technology/2010/aug/15/internet-brain-neuroscience-debate. Accessed 25 June 2017.

Neumark, F. (1970). Grundsätze gerechter und ökonomisch rationaler Steuerpolitik. Tübingen.
Pyka, A. & Andersen, E. S. (Eds.) (2013). Schumpeter's core works revisited. Resolved problems and remaining challenges. *Long term economic development, economic complexity and evolution* (pp. 9–31). Springer-Verlag. doi:https://doi.org/10.1007/978-3-642-35125-9_2
Smith, A. (1776). *An inquiry into the nature and causes of the wealth of nations*. London: Methuen & Co., Ltd.
The Financial Complexity Index. 2017. https://www.tmf-group.com/en/news-insights/publications/2017/financial-complexity-index-2017. Accessed 4 Aug 2017.
UK Government. (2017). https://www.gov.uk/government/publications/making-tax-digital/overview-of-making-tax-digital#next-steps build by the Government Digital Service. Accessed 1 July 2017.
Vero.fi. (2017). Incomes register. Finnish Tax Administration's website. https://www.vero.fi/en/About-us/information_and_material_on_taxatio/incomes-register. Published 5/15/2017. Accessed 1 July 2017.
Wagner, A. (1880). Finanzwissenschaft, Gebühren und allgemeine Steuerlehre. In: A. Wagner & E. Nasse (Eds), *Lehrbuch der politischen Ökonomie* (6. Band, 2. Teil, S. 220 ff). Leipzig/Heidelberg.

Welfare in a Competitive European Union? Some Aspects of Cybernetic Higher Education (HE) Policy in Knowledge Generation

7

Kajetan Stransky-Can

Contents

Abstract

In Neoclassic Economic Growth Theory, economic growth (g) is co-determined by (investment into) Research and Development (R&D). Considering the background of a simple production function of the European companies including R&D as an enhancing factor of capital and labor, the European Union (EU) is seen as a region where this causality is relatively strong in comparison to regions where the effects of g are predominantly determining resource flows into R&D. This analysis attempts to discuss Higher Education (HE) Policy – facilitators for investments into R&D (the view of Growth Theory) and examples of this kind of investment into basic and applied research in Austria. Another example of an established facilitator for investments into R&D is the knowledge transfer from (the escalation of) national HE Policy programs to a supranational level (e.g., the EU Framework Programme for Research and Innovation). We also take a look at the feedback from g on resource flows into R&D (the view of Knowledge State Theory), since

This analysis is based on the cited literature, personal reflections of the author and comments of a reviewer only and does not necessarily reflect on positions of the Austrian Federal Government.

K. Stransky-Can (✉)
Bundesministerium für Wissenschaft, Forschung und Wirtschaft, Vienna, Austria
e-mail: kajetan.stransky-can@bmwfw.gv.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_45

especially basic research funding is expected to be predominantly input-based (i.e., government expenditure stocks are path dependent and changes in expenditure stocks depend on g through overall government revenue). This feedback-loop is considered as a main element of Cybernetic HE Policy. However, it is clear that g is a much larger aggregate of processes than public, private, or public–private-partnership (PPP) R&D. As a last step, findings from an analysis of consequences of (PPP-induced) quality management in Austrian HE institutions for the academic profession will be reflected on grounds of the findings about aspects in Organizational Sociology and EU – member state observations.

Keywords
Knowledge state · Research and development (R&D) · Basic research · Applied research · European Union · Austria · Supranational politics · Knowledge democracy · State funding · Higher education policy · National politics

Introduction

Government policies in states of the European Union (EU) are increasingly recognizing Research and Development (R&D) as an important factor of economic growth (g) of Gross Domestic Product (GDP) (Campbell 2006, p. 26). G is an input factor of income and wealth creation and, through taxes on household expenditure and investments, indirectly on government revenues. Also, government expenditure (G) plays a vital role for R&D (e.g., Etzkowitz and Leydesdorff 1997, p. 2). The feedback loop between g and R&D can be seen as an important cybernetic element of Higher Education (HE) Policy. Additionally, we can differentiate between basic and applied research. Hereon, two examples of the Austrian R&D-system will be portrayed: a company performing Mechatronics and a research institute in the scientific field of Physics.

The government role in liberal democracies in HE Policy is determined by both macro- and microeconomic circumstances (Baumeler 2009, p. 69): Relatively high rates of g are reflecting international competitiveness of an economic area; according to Neoclassic Economic Growth Theory (Solow 1956), GDP is created by firm input factors of labor (l) and capital (c), which both can be enhanced by a factor of R&D. In economic areas such as the EU, where GDP is relatively high, the main advantage of the GDP-enhancing factor of R&D in contrast to l and c is its nondeclining marginal revenue, that is, more input of R&D in any state of production is yielding (at least) the same additional revenue. In contrast, in economies at a lower level of development, the production factors of l and c are yielding relatively more additional revenue. Then, g should be high enough to handle R&D as a selective policy field and in liberal democracies; large companies have played an important role in (applied) R&D traditionally (Noort 2014, p. 14).

The nondeclining marginal revenue of R&D, though, is one justification for policies aiming at the creation of "Knowledge States." Campbell (2006, pp. 26–27) describes the following elements as their features (elements of "Wissensstaaten"):

a) Politics acknowledges the status of knowledge for society, democracy, and the economy.
b) Politics aims at supporting knowledge.
c) With Knowledge and/or Innovation Policies, politics wants to support the economic development by distributing societal knowledge to economic actors.
d) In a cybernetic sense, economic development is also serving the societal knowledge stocks.
e) Noneconomic targets are also included into Knowledge and/or Innovation Policies.

In this analysis, indication from the literature on HE Policy for both sides of the feedback mechanisms concerning R&D and g will be presented. The case of Japan should show that drawing conclusions for government policies from an analysis of this interplay is not straightforward: In this country, relatively high investments into R&D (Campbell 2006, pp. 32–34) did not automatically lead, at least in the past two and a half decades, to sustained economic growth. The description of the interconnections between R&D and g will not be reflected on their socio-historical background here, but rather on some aspects of the current role of G in operative R&D.

Feedback from Research and Development on Economic Growth

A substantial role of Research and Development (R&D) in the processes of creating welfare can be described by the aggregated statistics of Gross Domestic Product (GDP), including the outputs of each individual production function from firms. Some effects of G onto R&D will be described in section "Feedback from Economic Growth on Research and Development (Via Government Expenditure)." Note that GDP is not able to measure overall welfare of a society. Obviously, these functions are directly influenced by R&D: The production factor labor (l) is partly constituted of academics; machines engineered in a Public–Private-Partnership (PPP) cluster could be a part of the production factor capital (c). In Austria, GDP in 2015 amounted to €340 billion (resulting in €39,390 per capita, see http://www.statistik.at/web_de/statistiken/wirtschaft/volkswirtschaftliche_gesamtrechnungen/index.html, accessed 21 July 2016), whereas in the same year, the 28 countries of the EU had a cumulated GDP of €14.6 trillion (http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=nama_10_gdp&lang=en, accessed 21 July 2016). Thus, the contribution of Austria to the economy of the EU-28 makes up to 2.3% with a population share of 1.7%.

In addition to performing (basic) R&D, universities themselves constitute an economic force, employ many people, and form communities by culture and style (Daxner 2010, p. 21). For the institutional interpretation of all these functions, the policy autonomy design shaped by Higher Education (HE) Policy is highly relevant. Policy autonomy is here understood as the opportunities of individual HE institutions to design their structure of staffing, whereas HE Policy is used when talking about the steering regime of a HE System designed by the state as one key actor. The

design of HE Policies in four European countries will be the topic of an authors' further publication on analyzing the strength of the paradigms of New Public Management (NPM), Network Governance (NG) (these terms will be explained subsequently), or a possibly newly emerging paradigm. The general term of institutional autonomy could also mean that policy-making institutions expect universities to play instrumental roles in developing and innovating nations or regions (Nybom 2014, p. 25).

Under the header of international competitiveness, reforms of industry-oriented Research Policy have been shaped by the European Economic Community (EEC) "Acte Unique," enacted in 1986. Here, specific programs were organized within a framework program to influence relationships between governments, HE institutions, and industry (Larédo 1997, p. 34; an example of a national government-supported cooperation between universities and industry in Austria will be given subsequently in this section). The introduction of Framework Programmes at a European level has happened at the same time where a vivid discussion of the role of political – or state – authority in state levels, HE institutions (HEIs), and business conduction has been led under the term of NPM. Hence, business administration principles gained influence in public administration and HEIs by introducing elements of Economic Policy making into HE Policy.

In any case, the European initiative of designing framework programs could be seen as an early attempt to many processes "where political authority is transferred upward, downward and sideways" (Abazi et al. 2010, p. 39): upward, because the Politics shaping Research Policy has been transferred to a European level. With Abazi et al. (2010, p. 40), we can add to the framework programs that "with increasing European influence in higher education (Lisbon agenda, Bologna process), authority tends to shift towards the supranational and intergovernmental levels." Downward, because HEIs, primarily universities, were given a higher degree of autonomy: "[HE institutions are characterised by] [i]nstitutional autonomy as a principle, whereby institutions act as enterprises but not as businesses, that is, they enjoy autonomy to high degree without tight leadership and a chain of command to the government" (Daxner 2010, p. 16, highlighting by KS). And sideways, because political authority is manifested in resources coming from government expenditure (G), from the private sector, or from both.

Returning to the case of European Research Policy, evaluation showed that the primary aim of the 1986 framework program, namely, changing the competitive positions of the participating firms, was not fulfilled. Rather, it had influence on the conditions for internal technological capabilities-development (Larédo 1997, p. 39; it might be useful not having fostered EU-internal competition here since the largest part of trade flows stays within the EU.) This conclusion could be interpreted as a sign of prevailing research specializations of applied research in the private sector and basic research in the HE sector in Western Europe of the 1980s.

Reflecting the need of public action in basic research, accompanied by an ongoing transfer in sources of political authority to a European level, a powerful instrument of European Research Policy added to the framework programs is the

European Research Council (ERC) grants. The ERC has been established "by a handful of independent and innovative European research foundations and Academies of Science, in spite of fairly heavy resistance" (Nybom 2014, p. 28) and reflecting a combination in European HE Policy of NPM principles such as evaluation for budgets with bottom-up friendly governance approaches such as the support of self-steering and self-organization in HEIs. From a European Politics perspective, it could be interesting to find out more about the sources of this resistance – which were the opposing actors, from which member states were they coming? However, the answers to these questions would be, from a perspective of forming expectations of HE actors, it is likely that established long-term EU-programs in research are advantageous in being relatively independent of national austerity measures (e.g., the Spanish National Research Council got 39 Starting and Advanced Grants from the ERC by the beginning of 2015). Ideally, there would be national support by an extensive investment path into basic and applied research. As Economic History has documented, this has also been an approach in semi-authoritarian, US-inclined emerging markets.

From a Comparative Politics view, it can be stated that the mixture of top-down and bottom-upapproaches to HE governance through ERC-instruments is relatively independent of national public administration action in HE Policy. This kind of governance might reflect an intensifying momentum for HEIs in strengthening their dominant position in national HE Policies, introducing a kind of NG. It is also expected of public administration sooner or later being influenced by NG-approaches in HEIs and business. Note, especially in terms of evaluating policy initiatives with differing focuses in applied or basic research, that the reception of an ERC-grant as a special kind of P&P-financing requires detailed evaluation (Jansen et al. 2007).

As the examples of the EU – framework program and the ERC show, there are different peer groups assessing the quality of research in a project established by resources from the first or the second: Whereas the peer community comes overwhelmingly from companies when assessing applied research, the peers in the ERC-assessments are coming from the academic community (an example of an Austrian research institute being successful in gaining ERC-grants will be outlined in the next section).

As a company, the Austrian competence center for excellent technologies "Linz Center of Mechatronics" gets its feedback from other companies. Microsoft is an example (http://www.lcm.at/microsoft-indoor-localization-competition-2016-vienna/, accessed 21 July 2016) where there is knowledge demand for a project in underground mining safety: "The surroundings of underground mining machines represent a hazardous zone for miners due to bad visibility conditions for the engine driver. Within the EU-funded project FEATureFACE, we have developed a prototype system for the estimation of the miners' positions around a machine employing time-of-flight measurements based on audible sound signals" (http://www.sciencedirect.com/science/article/pii/S0003682X14003168, accessed 20 July 2016). The application has already been successfully tested and represents an alternative to the electro-magnetic location systems used up to now (http://www.lcm.at/forschung/internationale-

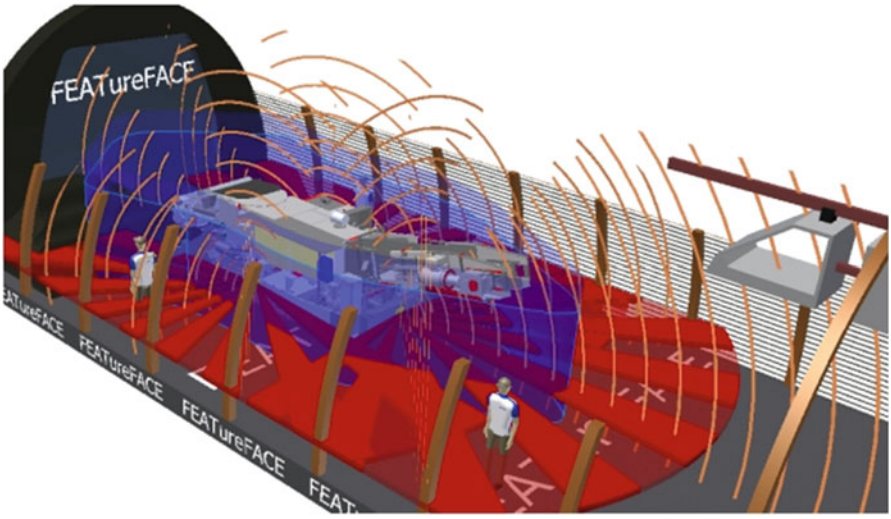


Fig. 1 Illustration of a sound based location system (Source: http://www.lcm.at/forschung/internationale-projekte-eu-projekte/, accessed 20 July 2016)

projekte-eu-projekte/, accessed 21 July 2016). The involvement of the Universities of Linz and Innsbruck and the University of Applied Sciences Upper Austria underlines the embeddedness of the "Linz Center of Mechatronics" into the Austrian knowledge system, and there are also many HE institutions from abroad engaged as cooperation partners (http://www.lcm.at/forschung/k2-projekte/partner/wissenschaftliche-partner/, accessed 21 July 2016). Besides the mentioned EU-sources, basic funding from the Austrian Research Promotion Agency (FFG) is substantial for the establishment of this competence center (Fig. 1).

Thus, we can see, already from the early EU-programs on Research Policy, effects from R&D on the microeconomic level of market-oriented private sector research. On a macroeconomic level, there is no obvious evidence for a dependence of g on R&D: Since the mid-1990s, growing tax transfers from EU-member states to the supranational level transformed into G have made the building up of institutions like the ERC possible. So, there is visible influence from the macroeconomic development of individual EU-member states such as Austria, Finland, France, or the UK. Note, however, that G for a supranational level might have been financed by growing depth rather than by favorable macroeconomic circumstances (see, e.g., the state crisis in Southern Europe in 2009 and the following years). But certainly, the advantage of established long-term EU-programs for research is that they are relatively independent of national austerity measures, as the case of the Spanish National Research Council shows. Therefore, economic growth is stabilized from a stock as well as from a flow perspective: G is stabilized as an input summand of GDP and R&D can continue to take its role in enhancing the input factors of l and c.

Feedback from Economic Growth on Research and Development (via Government Expenditure)

Especially in the area of basic research as a part of Research and Development (R&D), basic funding is directly contributed by the state or supranational institutions, for example, through government expenditure (G) in university accounts. For example, in 2014, an average Austrian university got between 85% and 90% of its turnover (directly or indirectly) from state funding (Bundesministerium für Wissenschaft, Forschung und Wirtschaft 2016). Furthermore, at least in Europe, national HE systems where basic funding plays an important role in public financing seem to be relatively successful, measured by frequently reported indicators (e.g., publications – Nybom 2014, p. 24). Normally, to bring this statement into a broader context and to paraphrase Esping-Andersen (1990), the higher the degree of state action, the more de-comodifying a nation state is. Note, however, that increasing institutional autonomy can also mean that universities can determine themselves the internal allocation of state funding, which does not have to mirror the budget calculating mechanisms used by public administration.

Also, G must be seen as an input into regulatory arrangements since public intervention plays an instrumental role for a growing number of collaborative arrangements in technology and research (Larédo 1997, p. 41). This tendency might be associated with the shutdown of large companies' innovation laboratories in many European countries, as the example of the Netherlands shows (Noort 2014, p. 14). In Higher Education (HE) Policy, we can see an ongoing discussion in diverse national contexts on the changing role of public administration from guaranteeing academic autonomy to taking increased steering action by setting incentives for network regimes (Ferlie et al. 2008). This steering might correlate with an introduction or an expansion of information technology (IT)-based controlling mechanisms such as quarterly reporting, as obligatory for Austrian universities (see (in German only), http://unicontrolling.bmwfw.gv.at/, accessed 22 July 2016).

Another country example, Finland, might have oriented itself towards Austrian legislation by introducing leadership elements into universities, but, however, without features of a tight leadership (Winckler 2014, p. 110). Larédo (1997, p. 38; highlighted by KS) points to an interesting cybernetic feature within the here outlined effect from G on R&D: "(Technological research) networks did not only build internal tools, but also promoted new norms or standards designed to 'organize' the market: (i.e.) networks of norms." As the above-described example of mining safety illustrates, it seems to have moved the technological frontier further to new security standards. The academic community engaged in those networks of norms is in a research project – oriented alliance with Network Governance (NG) – oriented actors from Economic Policies to strengthen its position in competition for public funding and at the academic market as providers of public and, also to a substantial degree today, private goods.

From the viewpoint of Politics analysis, a possible explanation why the hard elements of New Public Management (NPM) have not been implemented in HE institutions (HEIs) in full effect could be the following: Public administration in HE

Policies (in a sense of predominantly top-down orientation), which are in a process to transform into HE governance frameworks (with stronger co-operative elements), might have been confronted with declining legitimacy of pure NPM-orientation ("tight leadership") resulting from its stand-alone position compared to HEIs allied with NG-oriented actors in the Economic Policy-Subsystems. In other words, industry might have been the actor having influenced more flexible steering regimes in some European countries (some evidence on Austria and Finland has been outlined) than an expectation of top-down-fashioned HEI leadership has influenced steering regimes. From a Contemporary History point of view, it would be interesting to detect a starting phase of public administration moving to a NG-oriented mode of governance. A question for this kind of study might be whether there has been a blurring of the boundaries of HE Policies with their two-actor constitution to other actors and/or Policies and, thus, an integration of HE governance into Economic and/or Innovation Policies.

More direct forms of state intervention have played a role in supporting economically deprived areas or upgrading schools to a higher education status, at least in Western Europe, as a part of Economic Policy (Abazi et al. 2010, p. 40). An example for an institution traditionally oriented towards the regional environment is the University of Klagenfurt in Austria. Another direct form of (supranational) state intervention is the inflow of ERC-grants up to €2 Mio into HEIs via individual researchers, creating long-term possibilities for basic research by supporting the constitution of research groups. The University of Klagenfurt is the hosting institution of an ERC – starting grant in the field of Social Ecology.

One of the most renowned examples of research groups being successful in gaining ERC-grants in Austria is the Institute for Quantum Optics and Quantum Information (IQOQI) with their two research centers in Innsbruck and Vienna. It is constituted by ten research groups and two managing directors where the research groups are headed by their respective leaders. Basic research in Physics is the key source for application in data transportation, as the example of the research group of Quantum Optics in Space of the IQOQI shows (Fig. 2):

> [W]e propose performing quantum optics experiments in a ground-to-space scenario using the International Space Station, which is equipped with a glass viewing window and a photographer's lens mounted on a motorized camera pod. A dedicated small add-on module with single-photon detection, time-tagging, and classical communication capabilities would enable us to perform the first-ever quantum optics experiments in space. (http://www.iqoqi-vienna.at/home/research-groups/ursin-group/quantumopticsinspace/, accessed 20 July 2016)

From the basic research performed in space, the IQOQI-researchers define their target for application in IT security as follows:

> Within a decade, it will be possible to place sources of entangled photons on satellites, which will allow global quantum communication, teleportation, and perfectly secure cryptography. Quantum cryptography relies on quantum communication technology but its progress and future impact on secure communication will depend on new protocols such as, for example, quantum-cryptographic authentication and quantum digital signatures. (http://www.iqoqi-vienna.at/home/research-groups/ursin-group/quantumopticsinspace/, accessed 20 July 2016)

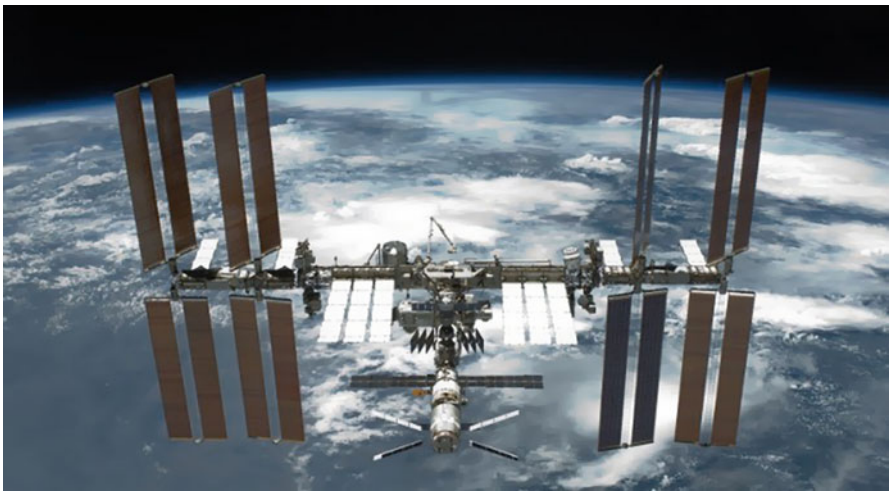


Fig. 2 The International Space Station (Source: www.htxt.co.za/2013/12/10/the-international-space-station-turns-15-today, accessed 20 July 2016)

The long-term perspective of such funding is a special feature of ERC-funding and supporting HEIs' autonomy, regardless of being a university or a university-oriented research institute such as the IQOQI (which is in a multi-faceted connection to the Universities of Innsbruck and Vienna). ERC-funding is especially important since, as Nybom (2014, p. 24) puts it, "most countries, turned from a system that included a lion's share of block grant funding into a system where time-limited 'competitive funding' has become the standard operating procedure." Campbell (2013, p. 213) shows that the competitive funding procedure might be interconnected with relatively lower job satisfaction rates in academic institutions (more about this point will be stated in section "Some Remarks on Government Expenditure in Operative Research and Development"). These points already show that there are no easily measurable effects of G on R&D, but as the paradigm of NG indicates, macro- and microlevel governance should be seen as interconnected and not solely as an issue for top-down decision.

Some Remarks on Government Expenditure in Operative Research and Development

Regarding again a micro- and a macrolevel, a number of government reforms in Europe where intended to increase the levels of competition between Higher Education institutions (HEIs) (and, of course, other publicly [co-]financed institutions) within a framework of constrained Fiscal Policy. From the 1980s onwards, public administration has been earmarked with the image not having dealt adequately with challenges national Higher Education (HE) Policies have been confronted with, such

as increased participation rates or a budget-overarching growth of scientific knowledge stocks. The reaction of public administration has been the introduction of New Public Management (NPM) – oriented reforms in HE Policies, possibly inspired by Economic Policy – actors (see also the discussion in section "Feedback from Economic Growth on Research and Development (Via Government Expenditure)"). The connection of performance with funding has reached an institutional level (Campbell 2013, pp. 205–206), meaning HEIs. As providers of (still) mostly public goods, they have to choose whether to interpret the reforms in their own way or to wait passively for further reform. Most HEIs take the first option; its usage is correlating with the expansion of an academic market by intensifying their role in provision of private goods from research and teaching.

However, the evidence concerning the effectiveness of NPM-reforms onto output of academic work is mixed – for example, Austria ranks relatively low regarding peer-review and article output (ibid., p. 211) even though it is a country where the NPM-guided Universities Act (UG, in German: Universitätsgesetz 2002) has been implemented since 2004. The perception of top-down management style has also been confirmed by Austrian academic staff at HEIs (ibid., p. 213). As stated above, Austrian universities act in some aspects as enterprises, but maybe rather without "tight leadership" (university management boards are frequently facing challenges when trying to integrate business administration principles into expert organizations). With a reform path in HE Policy resembling to Austria, Finland is a country where similar elements to the UG have been implemented in HE Policy. However, it is France and the UK that can be seen as the first countries in Europe where "the governments aimed at making universities more accountable for the funding they received, but also restraining detailed regulation in favor of market-like mechanisms" (De Corte 2014, p. 133). This statement is underlining the thesis of HEIs acting on an expanded academic market. It is further evidence for a changing character of the supply in outcomes of academic institutions towards the private goods – idea.

In any described country case, we can speak about liberal democracies. Campbell and Carayannis (2012b, p. 19, highlighted by the cited authors) describe the connection between developments in the economy and those in democratic processes as follows:

> *Between processes and structures of advanced knowledge democracy, knowledge society, and knowledge economy, there is a certain congruence [. . .].* Concepts of democracy (moving from electoral to liberal and high-quality democracies), and of knowledge and innovation [. . .] are becoming broader and increase their complexity considerably. *Political pluralism in democracy cross-refers to creativity-encouraging heterogeneity and diversity of different forms, modes, and paradigms of knowledge and innovation.*

Therefore, Campbell and Carayannis (2012b) help in reflecting the economic theory of Solow (1956) being the starting point for the understanding of economic growth (g) within this chapter: The citation is underlining that R&D should neither be seen as a black box nor that it is an economic factor being independent of society and democracy.

For further research, it could be interesting to ask whether the Politics generating HE Policy have changed in the mentioned countries under changing macroeconomic conditions such as reduced g. In particular, there could be cybernetic elements in the interaction of key topic specialization patterns in Government Expenditure (G) and Research and Development (R&D).

Another aspect concerning primarily a microeconomic perspective is the individual researchers' situation. Considering the example of the ERC-grants, the academic quality of research proposals is evaluated by peer-review, leaving the negatively evaluated researches without any granting from this source. Of course, institutional support in staff and/or infrastructure for getting the ERC-support would have been classified as sunk costs. Here, also the feedback-mechanisms between researchers and evaluators form an academic market, creating market-similar principles in connection with legitimating the use of supranational resources by a high entrance barrier (i.e., passing the evaluation). Academic markets are, therefore, suited for institutional as well as individual interaction. A country where we can find an example of institutional funding dependent on a hard-accountability evaluation system is the UK with its Research Assessment Exercises (RAEs) (ibid., pp. 207–208). As indicated above, the UK has been among the first movers in introducing NPM into HE Politics. There were possibly drawbacks onto strategies on the suprainstitutional level such as the EUA (European University Association) or onto regional policy in local territories of the UK or other countries, being relevant for analysis in Political Science. An investigation of the transformation of HE Policy within HEIs, especially of changes in the organizational structure, could be interesting from a viewpoint of Sociology.

Conclusion

As this analysis is rooted in an interdisciplinary area spanning from Political Sciences to Economics, we can sum up that Knowledge States are generally supporting basic and applied research. In a familiar understanding of the term of a Welfare State (Esping-Andersen 1990), it is more probable that current economic growth (g) and forecasts of g are determining resource flows into R&D. Examples of state (Knowledge State) action in Austria are the "Linz Center of Mechatronics" with a focus in applied research and the Institute for Quantum Optics and Quantum Information, oriented towards basic research. The patterns of supporting research depend, however, on paths of institutional development on state level and the interaction of political actors on a supranational level. In addition to Austria, Finland seems to move on a similar reform track, whereas France and the UK can be declared as early movers concerning New Public Management (NPM)-oriented reforms in HE Policy. On an EU-level again, strong features of Network Governance (NG) can be found when we take a look at the European Research Council – grants. Furthermore, g feeds back on the possibilities of Higher Education (HE) and Economic Policies. At the same time, these Policies are a prerequisite for the key actors' interaction in those fields and, therefore, shaping the position of HE institutions (HEIs) and companies (Fig. 3).

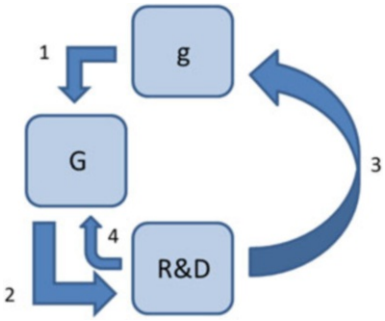


Fig. 3 An example of cybernetic interactions between *g*, *G*, and *R&D* (Source: authors' own (*1*) Economic growth (*g*) is determining government expenditure (*G*). (*2*) Government expenditure (G) is an input into Research and Development (R&D). This holds true for the basic as well as the applied research (examples from Austria, presented in section "Feedback from Economic Growth on Research and Development (Via Government Expenditure)," are the "Linz Center of Mechatronics" and the Institute for Quantum Optics and Quantum Information). (*3*) Research and Development (R&D) is a condition for economic growth (g) as an input enhancing the production factors of labor and/or capital. Of course, it is also an important factor in further social processes that form liberal democracies (Campbell and Carayannis 2012b). (*4*) Research and Development (R&D) is creating norms used by the state and, therefore, contributing (ideally) to a ceteris paribus – budget increase via cost-reduction, that is, a direct redistribution from R&D-induced cost reduction into government expenditure (G) for R&D.

For further discussion, three critical points are highlighted here:

- Within the cybernetic interaction forms of Research and Development (R&D) and g, further cybernetic mechanisms seem to work within the networks and clusters forming the two directions of correlation (see the example of government expenditure [G] helping to create public-private partnership projects which generate new norms used by the government). Economic growth is not the sole factor of welfare creation – see, for example, the presented findings on working conditions in academia.
- Considering less the field of Economic Policy, but more with a focus on specific HE Policies, the conglomeration of the EU has to be disaggregated for further analysis as differences between member countries in turns of practical consequences of New Public Management (NPM)-inspired reforms seem to be remarkable. Austria and France as countries located in continental Europe and Finland and the UK as countries located in northern Anglo-Saxon Europe, respectively, could serve as examples for research.
- The consequences from state organization for institutional steering have to be further investigated when we take a look at the patterns of research in HEIs (e.g., institutional profiles in basic or applied research specialization). The generation of hypothesis on developments of disciplinary formation, directly or indirectly influenced by HE Policies, could be interesting.
- Within this context, HE Policies could be seen as shaped by political narratives such as NPM and Network Governance. Attributes of both of those narratives

(see Ferlie et al. 2008, pp. 335–336; Campbell and Carayannis 2012a, p. 48) such as the stimulation of competition for research funding, stronger managerial roles by senior academics, a substantial self-organizing capacity, and elements of team-based approaches can be found in research groups founded by the European Research Council such as the Austrian Institute for Quantum Optics and Quantum Information. University management layers are aware of those bottom-up-combinations of narratives, which seem to reduce their political connotations when applied in daily research activities. The challenge remains, however, to combine the meaning from outcomes of these activities with pure top-down approaches to Governance and University steering. A solution could be the clear manifestation of an activities profile and a discussion on quality assurance, enhancement of management mechanisms in HEIs in a participative way.

References

Abazi, A., Farrington, D., & Huisman, J. (2010). Globalisation, internationalisation and regionalisation. In J. Huisman & A. Pausits (Eds.), *Higher education management and development*. Münster/New York/München/Berlin: Compendium for Managers.

Baumeler, C. (2009). Entkopplung von Wissenschaft und Anwendung. Eine neo-institutionalistische Analyse der unternehmerischen Universität. *Zeitschrift für Soziologie, 38*(1), 68–84.

Bundesministerium für Wissenschaft, Forschung und Wirtschaft (Federal Ministry of Science, Research and Economy). (2016). University Accounts. https://oravm13.noc-science.at/apex/f?p=103:2::REFRESH_TREE:NO::P1_TREE_ROOT,P2_TREE_STYLE,P1_SELECTED_NODE:166,BAUM,166. Accessed 14 Jan 2016

Campbell, D. F. J. (2006). Nationale Forschungssysteme im Vergleich. Strukuren, Herausforderungen und Entwicklungsoptionen. *Österreichische Zeitschrift für Politikwissenschaft, 35* (1), 25–44.

Campbell, D. F. J. (2013). New university governance: How the academic profession perceives the evaluation of research and training. In U. Teichler & E. A. Höhle (Eds.), *The work situation of the academic profession in Europe: Findings of a survey in twelve countries; The changing academy – The changing academic profession in international comparative perspective 8*. Dordrecht: Springer.

Campbell, D. F. J., & Carayannis, E. G. (2012a). *Epistemic governance in higher education: Quality enhancement of universities for development*, *Springerbriefs in business*. New York: Springer.

Campbell, D. F. J., & Carayannis, E. G. (2012b). *Knowledge production in quadruple helix innovation system: Twenty-first-century democracy, innovation, and entrepreneurship for development*, *Springerbriefs in business 7*. New York: Springer.

Controlling in Austrian Universities. http://unicontrolling.bmwfw.gv.at/. Accessed 22 July 2016.

Daxner, M. (2010). Understanding higher education management. In J. Huisman & A. Pausits (Eds.), *Higher education management and development*. Münster/New York/München/Berlin: Compendium for Managers.

De Corte, E. (2014, November 6–7). Quality assurance and university governance: Complementary activities. Österreichischer Wissenschaftsrat. Wohin geht die Universität? Quo Vadis, Universitas? Tagungsband 2014. Vienna: Annual International Conference of the Austrian Science Board Location.

Esping-Andersen, G. (1990). *The three worlds of welfare capitalism*. Princeton: Princeton University Press.

Etzkowitz, H., & Leydesdorff, L. (Eds.). (1997). *Universities and the global knowledge economy: A triple helix of university-industry-government relations*. London/Washington, DC: Cassell Academic.

Ferlie, E., Musselin, C., & Andresani, G. (2008). The steering of higher education systems: A public management perspective. *Higher Education, 56*, 325–348.

GDP on Austrian and European Levels. http://www.statistik.at/web_de/statistiken/wirtschaft/volkswirtschaftliche_gesamtrechnungen/index.html and http://www.lcm.at/forschung/internationale-projekte-eu-projekte/. Accessed 21 July 2016.

Jansen, D., Wald, A., Franke, K., Schmoch, U., & Schubert, T. (2007). Drittmittel als Performanzindikator der wissenschaftlichen Forschung: Zum Einfluss von Rahmenbedingungen auf Forschungsleistung. *Kölner Zeitschrift für Soziologie und Sozialpsychologie, 59*(1), 125–149.

Larédo, P. (1997). Technological programs in the European Union. In H. Etzkowitz & L. Leydesdorff (Eds.), *Universities and the global knowledge economy: A triple helix of university-industry-government relations*. London/Washington, DC: Pinter Pub Ltd.

Linz Center of Mechatronics. http://www.lcm.at/forschung/internationale-projekte-eu-projekte/ and http://www.lcm.at/forschung/k2-projekte/partner/wissenschaftliche-partner/. Accessed 21 July 2016.

Microsoft – Interested in Linz Center of Mechatronics. http://www.lcm.at/microsoft-indoor-localization-competition-2016-vienna/. Österreichischer Wissenschaftsrat: Accessed 21 July 2016.

Noort, E. A. (2014). "The World we live in 2014 – And beyond." The Universities and the Confluence of Internal and External Forces of Change. In Wohin geht die Universität? Quo Vadis, Universitas? Österreichischer Wissenschaftsrat, Tagungsband 2014. Vienna

Nybom, T. (2014). "The World we live in 2014 – and beyond." The Universities and the Confluence of Internal and External Forces of Change. In Wohin geht die Universität? Quo Vadis, Universitas? Österreichischer Wissenschaftsrat, Tagungsband 2014. Vienna.

Science Direct Article Abstract. http://www.sciencedirect.com/science/article/pii/S0003682X14003168. Accessed 20 July 2016.

Solow, R. (1956). A contribution to the theory of economic growth. *Quarterly Journal of Economics, 70*(1), 65–94.

Winckler, G. (2014). Autonomie und Governance. In Wohin geht die Universität? Quo Vadis, Universitas? Österreichischer Wissenschaftsrat, Tagungsband 2014. Vienna.

The Limits of European Integration Theories: Cyber-Development and the Future of the European Union

8

Thomas A. E. Fuchs

Contents

T. A. E. Fuchs (✉)
Political Science (Research Focus: European Union, European Integration), University of Vienna, Vienna, Austria
e-mail: thomas.a.e.fuchs@gmx.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_62

Abstract

This analysis attempts to explain the current state of the European Union after the Treaty of Lisbon, as the last great Integration Process. The author tries to answer the question, whether the National States or the Institutions of the European Union are the Global Players in the political decision-making process. The institutions, norms, and content of the contracts are in focus of this polity-based analysis. It should also supply sufficient information, if static-oriented Integration Theories are still state of the art. Or does the ongoing development process of the European Union ask for a different kind of Knowledge Development? The main aim is to develop new knowledge on thinking how the future of the European Union could look like and to build bridges between different views of how responsibilities should be divided between the Member States and the Institutions of the European Union. Is the White Paper of the European Union the right answer on how to deal with future challenges in the world of Cyber Development?

Keywords

European integration · Neo-functionalism · Liberal intergovernmentalism · Treaty of lisbon · Cyber development

Introduction

European Integration is a current and ongoing issue. Since the Constitutional Convention in 2002, it has created the impression that the process is only conducted in the form of compromises and without concrete objectives. After the ratification process of the Treaty of Lisbon, the European Union is under permanent pressure in the form of numerous crises. It seems as if a pure uncontrolled and desperate preservation of the current situation prevails since the financial crises in 2008. In 2015, when more than one million people flew from war in Syria there was also less intention for a global solution. From the beginning, Hungary and Poland have expressed themselves clearly that they do not want to cooperate in a unified solution. The BREXIT showed the fact that a European sceptic movement was generated, which becomes stronger in many Member States. It looks like Europe is split in two different convictions – on the one hand, the National States which should solve the European problems bilaterally and on the other hand a unified solution by the Institutions of the European Union. This analysis should show how the European Integration could be better explained. Finally, the result should reflect how the analysis could relate to further Cyber Development (Carayannis et al. 2014).

Research Question

The year 2017 marked the 60th anniversary of the European Project. It should be a year of celebration but the Union is maybe more in a crisis than in good shape. The European Integration project stagnated and the Member States are pursuing their

own paths. Easy solutions are propagated on big globalization problems. This analysis will deal with European Integration. Up to the European Constitutional Conference in 2002 and 2003, it might feel that European Integration has been a continuous and ongoing process since the creation of the European Coal and Steel Community. Of course, there were also small setbacks, for example, when Charles de Gaulles, with the so-called government without a chair, blocked the decisions in the Council. It was the discourse in the 1960s, which led people like Stanley Hoffmann to think about a purely institutionalist view (see Hoffmann 1964, 1966). Up to this event, the Neo-functionalist theory explained how European Integration worked. Rationalists, or rather neo-rationalists, provided new insights for grasping European Integration. They believed that persistent spillover effect came to a standstill. Compared to then, the actual problems of the European Union may be much greater. Since the Constitutional Convention, this has been confronted with setbacks in the field of integration. The proposed Constitutional Treaty failed not least due the negative referendums in France and the Netherlands. It feels like the National States are increasingly determining the agenda of the European Union, not only in the European Council, in the direction and decisions of the Ministers of the Council, but also in the case of partial solutions outside the institutions of the European Union. Domestic political interests are the priority in the negotiations of the Member States. The only movement of power on a supranational level happens when it comes to the creation of "de novo" bodies. In the financial crisis, the European Stability Mechanism (ESM) and the European Financial Stability Facility (EFSF) have been installed; the Commission and the European Central Bank only act as observers (Bickerton et al. 2015).

This initial impression is to be taken and analyzed within this work. How could a research question dealing with European Integration now look like? After initial reflections, the author has decided to choose two research questions that will keep a current state of European Integration:

1. What is the current state of European Integration?
2. Is European Integration a continuing success or is it stagnating?

These questions are not intended to have a prescriptive character, but it is necessary to take a stock in the case of European Integration.

Relevance to Political Science

Research on the European Union may be a valuable contribution to Political Science in many discourses. Political Sciences at the University of Vienna has a major focus in compulsory core subjects and selectable specializations, which deal with the political system of the European Union. The integration process of the Union is currently obviously confronted with numerous problems, especially when there is no agreement at the supranational level. The financial crisis in 2008, which has not brought concrete solutions to date, and the further exacerbation caused by the refugee crisis in 2015, will

be mentioned here. The Maastricht Treaty has brought the European Union more and more into the domestic political affairs of the Member States; it should form a kind of new European Identity, remote from a purely national-oriented one. The European Union also became more tangible and receptive to criticism of globalization. Its goal is to solve major problems and is therefore responsible in case those remain unsolved. As already mentioned above, numerous Member States of the European Union are increasingly returning to find national solutions and suggests the incompatibility of a United Europe. For those reasons, research in the field of the European Integration process can be of great interest to Political Science, because they are trying to find new ways to uniting Europe and developing Knowledge Society.

Theory

European Integration is very well researched in the field of theories and therefore numerous literature exists on this subject. There is a very broad set of theories which aim to grasp European Integration, which are not only very comprehensive in terms of quality, but also in terms of quantity. One could describe this as a torment of choices. Which theory is best suited for a current inventory and to adequately cover the subject field?

The EU is, on the one hand, understood as a multilevel system that takes supranational, national, and subnational actors and institutions and, on the other hand, negotiates with each other as a system by rationalizing National States as rational actors in the sense of maximizing benefits (Hooghe and Marks 1996). To answer the research question best, integration theories should be defined, which can further explain whether the final decision-making power should lie by the National States and their governments or by institutions of the European Union. One of the most stringent dividing lines in the European Integration theories might be between Neo-functionalism and Liberal Intergovernmentalism.

Liberal Intergovernmentalism

Liberal Intergovernmentalism is a theory, which has a different point of view on the phenomena of European Integration and provides another explanation for it. This theory is about the question why are sovereign states ready to coordinate their central economic policies and give sovereign rights to international institutions.

First of all, Liberal Intergovernmentalism looks like a paradoxical combination of the two traditions of international recognition of liberalism and rationalism. The approach of Andrew Moravcsik is a new version of an intergovernmental approach. He rejects the functionalist theories and is oriented towards a realistic strand. This theory is a further development of intergovernmentalism. The key point is that the governments of the Member States are the main actors in the process of European Integration. Even when they delegate competencies to an institution like the European Union they were strengthened due to the fact that responsibility is

handed over. In that point of view European Integration advances when governments converge and pursue common goals. It stagnates when there is no consensus found in the negotiation. The funeral behavior is therefore always in the foreground. Andrew Moravcsik developed the theory further and gained dominance in the 1990s (Moravcsik 1998). His theory sees the governments of the Member States also as the key actors in the integration process, but not in a radical way. The theory of Moravcsik has also a liberal approach. A bottom-up perspective focuses on the different preferences of social actors that influence domestic power relations. Thus, the liberal approaches move to the fore. However, unlike constructivist approaches to Liberal Intergovernmentalism, as in rationalism, one sees individual treatment. It could also speak of intentional intergovernmentalism, which explains the interests and preferences of the actors. The actors are self-optimizing units, which also include the behavior of other actors. Liberal Intergovernmentalism could, however, be understood as a softer rationalism because it assumes that the actors are limited in their capacity to process information. At the international level, national governments could try to rationalize their preferences, but at the same time their rationality and aggregated interests are not always of the greatest use. What does this mean for European Integration? When does it happen from the point of view of Liberal Intergovernmentalism? Andrew Moravcsik formulates three basic concepts of a liberal theory for international relations. First, rational individuals and private groups are the central actors of international politics and not National States and institutions. The interests of these individuals are formulated in preferences and try to enforce them on domestic competition. The nature of the political system, as well as the distribution of power between the competing domestic actors, determines which interests ultimately influence the state preference formation process. Secondly, the state is not conceived as a single and autonomous actor, but is a product of social power relations. It aggregates the preferences of the key domestic political actors and implements them in state policy. Thirdly, political international interdependence comes to the fore. It is trying to enforce state preferences internationally. Of course, the behavior of the other states involved in the negotiation process plays a decisive role. Whether intergovernmental cooperation is the result of the negotiations depends on the interdependent interests concerned. Converging and complementary interests create incentive for cooperation and diverging interests prevent this. In simple terms, Liberal Intergovernmentalism is about negotiation and bargain between Member States. Moravcik's analysis perspective is chronological, which includes three stages. The first question is how preferences in the National States develop and whether they are influenced by economic or geopolitical interests. This is done with the aid of the liberal theory of preference formation, which in turn raises the question of how these preferences are implemented in intergovernmental negotiations. The Bargaining theory examines whether the results are explained by the negotiating power of the Member States or by supranational actors. Ultimately, the issue of Liberal Intergovernmentalism raises the question of why National States are giving their sovereignty to an international organization like the European Union. Is this step to be explained by a federal idea or by an interest of governments in binding agreements (Bieling and Lerch 2012, pp. 141–163)?

For the planned analysis, on the state of European Integration, it is not possible to address each individual analysis point. The Liberal Intergovernmentalism as a theory helps to explain those cases in the period between the Constitutional Convention and the Treaty of Lisbon, in which the National States continue to hold their power and sovereignty and are not ready to hand them over to an international institution. How the preferences were developed in the National States in advance will not be included in the analysis. The national actors are therefore not relevant. Liberal Intergovernmentalism is defined in this work as a contrast to Neo-functionalism because, even in the availability of interdependence between the Member States of the European Union, it does not lead to a distribution of competences and power but leaves it to the national government.

Neo-functionalism

Neo-functionalism is one of the most popular and oldest theories explaining the European Integration, in the 1950s and 1960s. This theory was mainly influenced by Ernst B. Haas, who wanted to find out the nature of this process. He is the most prominent neo-functionalist writer with his book: "The Uniting of Europe: Political, Social, and Economic Forces" (Haas 1958). Ernst Haas' Neo-functionalism is based on older theories of social science. Like Emil Durkheim, he sees that society is becoming more and more professional through the modern division of labor, but at the same time the interdependence also increases. This is happening across borders. In terms of intergovernmental relations, the focus is not on the interests and actions of national governments, but on the increase in interdependencies leading to the action of political actors. As a result, Haas sees integration as a process. The focus is on the cooperation of political actors, the creation of joint institutions which have a political relevance, and the associated transfer of power and loyalty.

He tried to avoid the weaknesses of older functionalism, in particular the separation of political and technical regulations in the cooperation of states. He retained the concept of gradual integration. Haas was especially interested in security and welfare gains through integration. As a starting point, ineffectiveness can be seen in politics because of insufficient integration. The functional spillover is about economics. The European Community would lose its legitimacy, if they do not generate common solutions in economic areas.

Spillover as an Engine for Integration

Neo-functionalism is focused on institutionalization of cooperation and no longer on networks of technical-administrative elites, like in David Mitrany's functionalism (Mitrany 1944). Both theories are about transferring sovereignty, loyalty, and power from the nation-state to new supranational communities. But there is one particular difference. The key message in functionalism theories is about the spillover effect. In contrast to Mitrany, Haas sees not only one but two forms. The first is like the old functionalism about the functional spillover, which is used to explain the way in which integration in one policy area creates pressure for integration in further areas. As a result of the above-mentioned interdependence by cross-border division of

labor, there is a need for cooperation between the actors. They help to build transnational institutions. According to Haas, cooperation is not limited to one area, but compels an expansive logic. If, for example, a cross-country cooperation between the coal- and steel-producing countries is established, then the working conditions and social standards of the workers will have to be considered, which in turn can lead to price fluctuations or have a bearing on transport costs. This again affects the regulations of the trucks, etc. An integrated integration project expands gradually, both functionally and territorially. It leads to the transfer of loyalty away from the National States to a supranational institution. For Haas, this transfer is not a prerequisite for successful integration, but a logical process. If the cooperation forms successful supranational institutions the views of national actors also will change. They will also be loyal to this institution. This effect describes the second and political spillover effect. The political spillover is used to explain the importance of supranational and subnational actors in the integration process, by increasing further pressure for more integration to pursue their interests. This process increases interdependencies and leads to a gradual surrender of sovereign rights. Pressure groups and political parties are also considered to be important actors. Because of these processes of spillover, neo-functionalists see European Integration as a self-sustaining process. For example, from free trade areas to custom union to single market to economic and monetary union and by an ongoing spillover maybe sometime a political union. Ernst Haas' definition of integration does not include a final goal setting, but he made a clear separation between supranational integration and simple intergovernmental cooperation (Bieling and Lerch 2012, pp. 55–77).

As mentioned above, Neo-functionalism experienced a certain setback, especially by Stanley Hoffman in the 1960s. It was shown that the assumption of Neo-functionalism, that the nation-states are continually giving up competencies in a two-stage spillover effect, does not always occur (Knodt and Corcaci 2012). There has not been a lasting spillover effect in many areas. If, however, the analysis moves on the desired polity level, the change in contracts existing up to 2007 shows a change in the distribution of competencies and also a gain in influencing the supranational institutions, like the European Commission and the European Parliament. For this reason, the Neo-functionalistic theory can be seen as a suitable counter-argumentation to Liberal Intergovernmentalism. Since not all aspects can be considered here, the analysis will not focus on regional and national integration processes. There will also be no separation between functional and political spillover. The Neo-functionalist theory will only help to work out those points of the process between the Constitutional Treaty and the Treaty of Lisbon, where there is a transfer from competences away from Member States to institutions of the European Union.

Research Design

What kind of research design could best answer the question already discussed, "What is the current state of European Integration?" As already mentioned in the theories, Liberal Intergovernmentalism and Neo-functionalism are likely to provide a good picture. However, in the case of research design it is imperative that decisive

concepts are defined. What is the best way to determine the current state of European Integration? It is possible to measure the arrangements within the Union on the basis of the last major and formative events. This is the financial and the refugee crisis. Only which standards could be measured here? In the area of the refugee crisis there were individual and group actions of National States, without a uniform line of the Union. This indicates an integration deficit, but does not show a clear pattern because of the lack of contractual arrangements. In the financial crisis, there were contractual agreements with the rescue package and the European Fiscal Compact, but these were related to the cause and with very little integration of democratic forces. The exact survey is likely to be very difficult and too complex. In the authors view, an ideal inventory for the scope of this analysis will be the last major contract agreement within the European Union. This is the Treaty of Lisbon, not just the content, but the way to the Treaty. This is not the long process of integration from the European Coal and Steel Community to the European Union but the last major phase of the Treaty. From 2002 to 2003, a common constitution for the European Union was created within the framework of the European Constitutional Convention. This failed and was somehow replaced by the Treaty of Lisbon. Just what were the exact reasons for this failure and what major changes are in this contract? The planned treaties of the Constitutional Convention and the changes that have led to the Treaty of Lisbon are defined as the concept of the current state.

The second concept is European Integration. How could it be defined for this work? In a certain way, European Integration could describe the visionary ideas of a time which have been formed on the continent following the catastrophic disillusionment of two world wars. This should never happen again and on this intention the course for peace in Europe was set. Last but not least, it was convictions that led nationalism to catastrophe, and peace could only be created and maintained under a common roof. These visions had characteristics ranging from a European federalism to a Europe of the fatherland, which continually changed. For this analysis, the concept of "European Integration" is to be defined as one which refers to the supranational level. It is progressing and increasingly developing in the direction to the United States of Europe and away from the National States. The power to determine the political agenda therefore lies primarily with the institutions of the European Union and not with the Member States. What would be the ideal survey method?

Method

Different methods were considered suitable, which were rejected later by the author. For example, this was an intergovernmental longitudinal analysis. It should refer to the period between the Constitutional Treaty and the Treaty of Lisbon and focus on the activities and interventions of the Member States. This form of analysis, however, would not lead to a comparison, but would lead to a purely rational, nationally oriented survey. This would be a descriptive hypothesis, in which no causality can be established. However, it would nevertheless meet the criteria of the clear definition

and possible falsifiability. The hypothesis would then be confirmed if, as a result of the analysis, it shows that for the process referred to, the National States have a higher influence on the definition of the political agenda than the institutions of the European Union. A comparative analysis between two integration theories appears to be more appropriate. This form of analysis would also raise the process from the draft Constitutional Treaty to the ratification of the Treaty of Lisbon as a longitudinal analysis of the time. Here, it makes the greatest possible use of theories, which differ fundamentally in their attempt to explain European Integration. On the one hand, there is a rational theory which sees the National States at the center of the European processes and, on the other, a theory which considers the institutions of the European Union to be an essential factor. From the outset, intergovernmentalism was firmly established as the theory which the nation-states regard as the centerpiece. It was less clear to find the most suitable theory for the supranational actors. Initially, a structure-oriented, federal approach, like multilevel governance, was favored. In contrast to a national-state theory, this would be the most remote from the basic principle and thus provide an excellent basis for comparison. Furthermore, the multilevel approach offers a theoretically good concept for the different stages of the system within the European Union, but it does not focus exclusively on supranational actors. Although the theory of Neo-functionalism has already been addressed, and has also been developed at a time when European Integration was completely different, it is a theory that focuses on when competences are handed over by the National States to other institutions. The aim of the intended analysis is not that the two spillover effects (functional and political) are separately collected and described, their exact causes for these effects, but in which areas the spillover effect in the desired analysis period took place. Therefore, this theory was chosen. The analysis is intended, with support of the Liberal Intergovernmentalism and Neo-functionalism theory, to show which competencies have been given to the supranational institutions of the European Union and in which areas the National States have retained their powers of attorney. This result is intended to illustrate the state of the European Integration process. It is important to note here that it is a declared goal of the analysis that neither the politics nor the policy level should be influenced too strongly. The process and the content for the negotiations will not be part of the full analysis, but will be briefly discussed. The relevant level is the polity level. The structures, norms, and forms of the institutions are to be raised in this analysis.

Hypotheses and Causality Analysis

As in the discussion of the method, it was not initially possible to decide what the ideal approach for answering the research question is. By a comparative analysis between two integration theories, causal hypotheses and thus causal connections can be established. For the first hypothesis, the independent variable would be the political agenda of the Member States of the European Union, and in the second, that of the European institutions in the European Union. The dependent variable in

both cases will be their influence on the European Integration. If the comparative analysis shows that the rational theory of Liberal Intergovernmentalism, and thus the National States more decisively, determines the policy of the European Union, the stagnation of European Integration would be confirmed.

H1 (Hypothesis #1): "The more the National States determine the political agenda of the European Union, the more European Integration stagnates."
H2 (Hypothesis #2): "The more the institutions of the European Union determine the agenda, the less European Integration stagnates."

Analysis

Starting Point Before the Constitutional Convention

The signing of the Treaty of Lisbon on 13th December 2007 by the Heads of State and Government of the then 27 Member States ended the debate on a Constitution of the European Union. Until that day, there was still the well-known three-pillar structure from the European Community.

A clearer allocation of the integration theories may have been still pertinent to the planned analysis. The First Pillar consisted of the European Community and the European Atomic Community as a supranational institution. The rights of sovereignty have been conferred and transferred to Community institutions. Thus, the first pillar was attributed to Neo-functionalism. While the second pillar, which includes the Police and Judicial Cooperation in Criminal matters (PJCC), and the third pillar of Common Foreign and Security Policy (CFSP) were more intergovernmental agreements. No sovereign rights were transferred to a supranational body, and sovereignty remained in the National States. Here the respective Member States had their own laws and processes. The second and third pillars were therefore intergovernmental cooperation. This pillar structure was to be dissolved with the planned constitution. A stronger supranational cooperation was sought. According to the defined concepts, this would mean that the path towards more integration should be created (Clemens et al. 2008, pp. 227–231).

From the Constitutional Treaty to the Treaty of Lisbon

History Seen with Both Theories

It might seem that since the European Coal and Steel Community has been founded in 1951, there is an ongoing process in European Integration which would not stop. In words of the Neo-functionalism integration theory, we would name this impression the so-called spillover effect. National States move their power systematic to a supranational institution – first to European Economic Community, then to the European Community, and finally to the European Union. Today we might have the impression that this process has stopped. The European Constitutional

Convention in 2002 and 2003 had one big goal to create a kind of European State, with a flag, a hymn, a symbol, and an own constitution, which includes a Charter of Fundamental Rights. This vision could not be fulfilled and therefore a comprise was implemented, the Treaty of Lisbon. Was this the death for European Integration?

The failure of a European Constitution was not just because of the two negative referendums in France and the Netherlands, but also of the doubt in many Member States. Since then the European Union has been in an integration crisis. The Treaty of Lisbon has taken many parts from the European Convent, but has not become the same. A document which was ratified as a compromised solution due to the failure of the Convent for a Constitution of the European Union. This event is a good example of the problems of European Integration process. The crucial point for the process of European Integration is one main question: What do the people of Europe want? Do they want an intergovernmental system, in which the National States still have the most political power in decision-making or do they want a multilevel governance system, in which supranational institutions like the European Parliament are the main actors? Is there even a possibility that visions from early twentieth century like a federal Europe still have a chance to come true? Let us take a look on the history seen by both integration theories.

Intergovernmental Integration Theory

If the process from the European Convention to the Treaty of Lisbon is seen in a realistic way like the intergovernmental integration model, then National States are the main actors. They have the priority to keep their national power and bring as much of their interests on the agenda as possible. So, in an empirical analysis the view will be on negotiation between the governments of the Member States (Clemens et al. 2008, pp. 309–310).

After the Treaty of Nice the European institutions wanted to create a constitution for the European Community with two main goals: first, to make the Union more efficient, democratic, transparent, and closer to the citizens and secondly, to define clear roles and responsibilities between the Union and the Member States. The Convention itself, under the chair of the former President of France Giscard d'Estaing, was composed of 15 governmental members, 30 members of national parliaments, 16 members of European parliaments, and 2 members of the Commission. Members of 28 National States, from them not all who were still in the European Union were represented. It seems these Member States tried to follow with the process.

Nevertheless, when it comes to the contracted agreement Spain and Poland did not sign. The explanation is that just the countries with high population like Germany, France, Italy, and Great Britain had favors with the votes in the Council of the European Union. In the end, Spain and Poland were successful. This point was changed and all Member States signed the contract on 29th October 2004 in Rome. Two negative referendums in France and the Netherlands followed. This is not just because of the problems in the domestic policy, but also due to the people's skepticism regarding the direction of European Integration. The fact that there will be a constitution, a flag, and a hymn nourishes the suspect that all Member States

will pass over in a European super state. Especially French citizens did not agree that Turkey should be a member of the European Union. After the failure of the constitution it was the Member States who essentially influenced the next steps in the debate of a new treaty. When the Treaty of Lisbon was signed on 19th October 2007 it was almost like a convention but essential parts were omitted. As a result, attributes, a flag, a hymn, a symbol, and a Charter of Fundamental Rights were not part of it. However, article 6 of the Treaty on the Functioning of the European Union grants the same legal liability as the contracts. But even there is an additional protocol which provides a special arrangement for the Member States Great Britain and Poland. The constitution wanted to grant many and specific rights to the national parliaments, but in comparison to the Treaty of Lisbon, the rights of participation of the national parliaments are still further developed. So, in an intergovernmental view the process between the Convent and the ratification of the Treaty of Lisbon was especially a main point where the Member States wanted to keep their power where it was. The European Union should not get attributes of a State. The Treaty of Lisbon also limits the competences of the Union and does not take the risk of undermining the national sovereignty of the Member States. This is clearly illustrated, for example, as the primary right of the European Union is established just in case where there is such kind of right. Otherwise the right is reserved by the Member States. Even the possibility of the return or reduction of competences which are already conferred on the Union is mentioned in the Treaty of Lisbon (Clemens et al. 2008, pp. 237–251).

As we know, the Treaty of Lisbon was not easily realized. It took two referendums in Ireland and a long process with the German Federal Constitutional Court.

Neo-functionalism

There is the idea that Member States will be linked to a whole, but in parallel maintain their own individual competences. They will not entirely arise in another level and stop existing. The European Convent was an attempt to get closer to a federalist continent. All of these points were in the Constitution of the European Union but as explained it was not ratified. Even though the Lisbon Treaty abandoned the goal of a Constitutional Treaty and abolished all existing treaties and replaced them by a real "constitution," it nevertheless took a few fundamental points within, which came close to the meaning of the Constitutional Treaty. The reform treaty cancelled the distinction between "Union" and "Community." It brought them together into one single organization and the unified name "European Union," excluding the European Atomic Energy Community.

According to the neo-functional view, there should be taken a look to which changes were made in the European Parliament, including members of the European Parliament itself. Maybe they are a major winner of the Constitutional Treaty. In the co-decision procedure, the European Parliament and the Council have equal opportunities, and it was extended to other areas and declared to a normal legislative process. For the proposal for the President of the Commission, the European Council should now consider the results of the European Parliament elections. Afterwards the

European Parliament had to elect the President of the Commission. The Lisbon Treaty has taken over these arrangements (Clemens et al. 2008, pp. 237–251).

Treaties and Law of the European Union

The treaty for a Constitution of Europe should replace the existing Treaties. In the end, the Treaty of Lisbon led to a change in the existing Treaties. The union law connected with it consists of primary law, international law, and so-called secondary law. The primary right includes the two main treaties, the Treaty on European Union and the Treaty on the Functioning of the European Union. Despite the established case law of the European Court of Justice that the right of union to be governed by the law of the Member States, this has not been expressly stated. This was not included in the Treaty of Lisbon from the Constitutional Treaty. However, it does not alter the fact that primary law and the powers conferred by the institutions of the Union in the exercise of the Union, the so-called secondary law, is over the law of the Member States. The entire national law of the respective National State, including constitutional law, is affected. This is due to the dissolution of the former structure and also for legal acts of the former second pillar "Police and Judicial Cooperation in Criminal matters" and the third pillar "Common Foreign and Security Policy."

Treaty on European Union

The Treaty on European Union (TEU) is one of the two main treaties of the Treaty of Lisbon. It consists of five titles with 55 articles preceded by a preamble. The common provisions should be particularly relevant to the analysis. The responsibilities between the European Union and the Member States are defined here. According to that, the EU is responsible only in those areas where their competences are clearly assigned. In those areas, which do not fall into the European Union's area of responsibility, the Member States remain fully empowered (Hellmann 2009, pp. 12–14).

Treaty on the Functioning of the European Union

Since the Treaty of Lisbon, the Treaty on the European Community has been called the Treaty on the Functioning of the European Union (TFEU). This is the reason for the merger of the European Community and the European Union, which now confers on the Union its legal personality. The Treaty complies with the principle of limited individual authorization, according to which the European Union is only responsible for the areas in which the Member States confer the competencies on it. The TFEU had the explicit objective of clarifying these competencies more clearly. In the case of these competencies there is a list of areas, in which the Union has exclusive, partial, and supporting competences (Hellmann 2009, pp. 12–14).

The areas, in which the Union has the exclusive competences, are the customs union, the establishing of the competition rules necessary for the functioning of the internal market, the monetary policy for the Member States whose currency is the euro, the conservation of marine biological resources under the common fisheries

policy, and the common commercial policy. These responsibilities are best explained by the Neo-functionalistic theory. In this area and for the conclusion of an international agreement, when its conclusion is provided for in a legislative act of the Union or is necessary to enable the Union to exercise its internal competence, or in so far as its conclusion may affect common rules or alter their scope the European Union has all the competences which were spilled over from the Member States (Consolidated version of the TFEU 2017, Article 3).

The partial competences are the internal market; the social policy, for the aspects defined in this Treaty; economic, social, and territorial cohesion; agriculture and fisheries, excluding the conservation of marine biological resources; environment; consumer protection; transport; trans-European networks; energy; area of freedom; security and justice; and common safety concerns in public health matters, for the aspects defined in this Treaty (Consolidated version of the TFEU 2017, Article 4).

The Union shall have competence to carry out actions to support, coordinate, or supplement the actions of the Member States. The areas of such action shall, at European level, be protection and improvement of human health, industry, culture, tourism, education, vocational training, youth and sport, civil protection, and administrative cooperation (Consolidated version of the TFEU 2017, Article 5).

So, the TEU and the TFEU cannot be exclusively explained neither by the Liberal Intergovernmentalism nor by the Neo-functionalism. This is because the competences are in some cases transferred to the European Union and in some cases, remain in the Member States.

The Union's Institutions

According to the Treaty of Lisbon, the European Parliament, the European Council, the Council, the European Commission, the Court of Justice of the European Union, the European Central Bank, and the Court of Auditors are the institutions of the European Union. By the dissolution of the pillar structure, the European Council became an own body. The organs of the European Union are a decisive factor for a normative political analysis and cannot be clearly assigned to neither the liberal intergovernmentalism nor the Neo-functionalism in its composition and its tasks. They must be individually analyzed and categorized (Consolidated version of the TEU 2017, Article 13).

The European Parliament

According to the Treaty of Lisbon, the European Parliament is the only body of the European Union elected directly by the Union's citizens. It fulfills, together with the Council, the task of legislation and budgetary powers. It also has a control function against the Commission and elects the President of the Commission by a simple majority. Thus, a decisive competence was conferred on Parliament. Not only in these tasks but also in the composition of a maximum of 750 MEPs is Article 14 of the TEU and Part I, Title IV, Chapter I of the Treaty establishing a Constitution for Europe consistent. However, the suggestion of the Constitutional Convention, for

a direct election of the President of the Commission by the European Parliament, was supplemented in the Treaty of Lisbon by a proposal of candidates by the European Council. The European Parliament is the institution, which enjoys a great independence factor from the influence of the governments of the national states, at least from a formal perspective (Consolidated version of the TEU 2017, Article 14).

The European Parliament could be most clearly associated with Neo-functionalism. It consists exclusively of elected representatives of all Member States and forms its own political groups. Since the Treaty of Lisbon, it has also been given a high level of competence with the function of legislator.

The European Council

By breaking the pillar structure with the Treaty of Lisbon, the European Council will become a separate institution of the European Union. It is composed by the Heads of State and Government of the Member States, the President of the Commission, the President of the European Council, and the High Representative of the Union for Foreign Affairs and Security Policy (under the Treaty for a Constitution for Europe, still EU Foreign Ministers). Its key task is to set up a high body to identify and act as the impetus for the development of the European Union and to define general policy objectives and priorities. The European Council's decisions are made in consensus and it does not act as a legislator. The TEU and the Treaty for a Constitution for Europe are also strongly similar in this case, as well as during the term of office of the President of the European Council of 2.5 years, with a re-election option in his election. The decision-making process is strongly influenced by the intergovernmental bargaining and negotiation fact between the Member States. The vote in the European Council takes place without the President of the Commission or the President of the European Council (Consolidated version of the TEU 2017, Article 15).

This institution can be seen by the Heads of State or Government of the Member States as an intergovernmental institution with a neo-functional influence by the President of the Commission and the President of the European Council. It should also be mentioned that the President of the Council shall not hold a national office.

The European Commission

The European Commission, with its many competencies, is a very powerful institution of the European Union and is particularly responsible for the implementation of the Union law. It is a control body with regard to compliance with the contractual provisions. Under the control of the European Court of Justice, the Commission supervises the application of the Union law. It sometimes also provides for the external representation of the European Union. It shall perform coordination, management, and administrative functions as defined in the Treaties. But the main competency of the Commission is the right of initiative, which usually emanates from the parliament in democratic systems (Consolidated version of the TEU 2017, Article 17).

Their tasks and composition are likewise strongly attributed to the theory of Neo-functionalism, due to the fact that they fulfill their activity independently of the

governments of the National States. Although one Commissioner is sent per Member State, the Treaty of European Union clearly states the independence of the act: "*The members of the commission shall be chosen on the basis of their general competence and commitment doubt. In charge of the Commission, the Commission shall be completely independent. Without prejudice to Article 18 (2), the members of the Commission shall not seek any government or other institution, body, office or entity. They shall refrain from any action incompatible with their duties or the performance of their tasks*." (Consolidated version of the TEU 2017, Article 17).

The Council

Until the Treaty of Lisbon the Council was still designated as Council of the European Union. The Constitutional Convention preferred the Council of Ministers (Article I-23 EVVA). It has the crucial competence to carry out the budgetary powers together with the European Parliament. The Council shall be composed of the various Ministers of the Member States and shall act by a qualified majority. The Council of "General Affairs" from the Constitutional Treaty was rejected again at the 2004 government conference; otherwise the ideas of the Constitutional Convention coincide with those of the Treaty of Lisbon (Hellmann 2009, pp. 39–41).

In addition to the European Council, the Council is a body composed of direct representatives of the national governments and shall act by a qualified majority. This form of decision-making requires a majority of 55% of the Member States, which must simultaneously represent 65% of the Union's population. The blocking minority of at least four members is intended to prevent the blockade of the population-rich Member States (Consolidated version of the TEU 2017, Article 16).

Negotiation and bargaining are very similar to the Council, and the Member States are clearly the global players in decision-making. It is thus most clearly attributable to Liberal Intergovernmentalism.

The Union's External Action

The High Representative of the Union for Foreign Affairs and Security Policy

Pursuant to Article 18 TEU, the Office of the High Representative for Foreign Affairs and Security Policy is hereby established. It does not constitute a separate body, but the office is exercised as part of the Union's organs. In accordance with the Treaties, the High Representative carries out the foreign and security policy together with the Member States (Consolidated version of the TEU 2017, Article 18).

Common Foreign and Security Policy (CFSP)

The common foreign and security policy is exercised by the High Representative as already mentioned, and by the Member States in accordance with the provisions of the Treaties. Pursuant to Article 21–46 of the TFEU, Member States fully support the CFSP in terms of mutual solidarity and loyalty. They do this in order to strengthen and further develop another. Furthermore, they abstain from any action which would

run counter to the interests of the Union or harm them in international relations. The Council and the High Representative are responsible for this. The European Council is responsible for determining the basic direction, as defined by the CFSP guidelines. On the basis of these guidelines, the Council shall adopt the necessary decisions (Hellmann 2009, pp. 73–79).

The Common Foreign and Security Policy is a strong intergovernmental institution. This makes the decision-making process clear. It is again based entirely on the principle of bargaining and negotiation. In principle, decisions are made unanimously, but there is the possibility of abstention. The decisions must then not be carried out by the Member State concerned but they are binding on the Union.

International Agreements

Pursuant to Article 47 of the TEU, the European Union has legal personality and is thus a derived subject of international law. The Union is thus capable of concluding international agreements with third countries and international organizations. Under Article 3 of the TFEU, the Union has exclusive competence to conclude international agreements, provided that the financial statements are provided for in a legislative act of the Union. Those agreements, which the Union concludes internationally, are binding on the institutions of the Union and its Member States (Article 216 TFEU). This rule corresponds in its widest to the rule already existing in the Treaty of the European Community (Article 300 TEC). The abstention of the vote in concluding international agreements does not release the Member States from implementing them (Hellmann 2009, pp. 80–84).

The area of the Union's external action is, on the one hand, a strong intergovernmental area in the field of CFSP, which, after the dissolution of the three pillars, has not fully developed into the competences of the European Union, such as the European Community and the police and judicial cooperation in criminal matters. Member States can have a strong influence through the Council and the European Council. The field of international conventions, on the other hand, has strong features of Neo-functionalism. While the decision is taking place at the Council, the competences are being pursued following the European Union, which negotiates binding agreements for the Member States. Here is a clear form of spillover.

Area of Freedom, Security, and Justice

The former second pillar, the police and judicial cooperation in criminal matters, no longer existed after the conclusion of the Treaty of Lisbon in its original form. The new area of Freedom, Security, and Justice includes the Policies on Border Checks, Asylum, and Immigration (Articles 77–80 TFEU), judicial cooperation in Civil Matters (Article 81 TFEU), judicial cooperation in Criminal Matters (Articles 82–86), and Police Cooperation (Articles 87–89 TFEU). The judicial cooperation in Civil Matters requires appropriate action to be taken by the European Parliament and the Council in the ordinary legislative procedure for the purpose of implementing judicial decisions between the Member States. The same is true of the

judicial cooperation in Criminal Matters. The principle of mutual recognition of judicial decisions and judgments applies. According to the principle of the ordinary legislative procedure, cross-border minimum rules can be laid down in certain areas of crime. These areas of crime are terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime, and organized crime. For the area of Police Cooperation, the Union shall establish police cooperation involving all the Member States competent authorities, including police, customs, and other specialized law enforcement services in relation to prevention, detection, and investigation of criminal offences. For these purposes the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may establish measures concerning the conditions and the application area (Consolidated version of the TFEU 2017, Articles 77–89).

The tasks of public policy and security remain the responsibility of the Member States even after the conclusion of the Treaty of Lisbon. The coordination of different forms of cooperation is free to the Member States. There are only a few forms of supranational integration. However, through the possibility of the ordinary legislative procedure, which is carried out by the European Parliament and the Council, it is possible to take binding decisions. The former pillar has also emerged in the European Union and does not have a special status like CFSP. The competencies are very much with the institutions of the European Union.

Causal Analysis

According to the research question: "What is the current state of European integration?" it can be said that neither the Institutions of the European Union, especially the European Commission and the European Parliament, nor the governments of the Member States are the only actors in the policymaking process. But also, the second question about the integration process cannot be answered clearly.

Referring to the examination of the causal state of the presented hypotheses, which independent variable now has the greater influence on the dependent variable and thus on European integration, it was showed that the process and the results cannot be mashed and seen together as one thing. The analysis can be split in three explanation patterns.

First, the intergovernmental view is maybe the better theory to explain the negotiation process between 2002 and 2007. National States are still important actors in European Integration process. The realistic content makes clear that National States are still global players who determine the agenda. All the changes, which were made after the Convent, were implemented to keep their power. The Constitutional Treaty would have provided much greater and far-reaching integration steps. The national governments, however, tried in many ways to enforce their own national interests. Here it is worth mentioning the example of Spain's and Poland's claim to adjust the voting modalities in the Council. Also, the fact that the Charter of Fundamental Rights is not fully incorporated in the Treaty of Lisbon is

due to the negotiation of National States. First United Kingdom and Poland and later also the Czech Republic claimed exemptions, so-called opt-outs, in the treaty negotiations regarding the legal claim of the Charter of Fundamental Rights.

Second, there are results which can be seen with both theories. The part in the Treaty of Lisbon, in which the competences are organized based on the distinction between competencies of the Union and the Member States, should be noted. The Treaty distinguished three types of competences. First, there are exclusive competences of the Union like the customs union, the competition policy, and the monetary policy. Second, there are shared responsibilities between the Union and the Member States like agricultural, energy, transport, and environmental policies. And third, the Union can make measures in support, coordination, and supplementary questions.

The institutions have defined clear tasks, which have intergovernmental and neo-functional elements too. On the one hand, there are strong competencies in supranational institutions. The European Commission and the European Parliament are key players in the submission and adoption of legislation in the field of secondary Union law and are only under a minor national influence and close to Neo-functionalism. On the other hand, the European Council, with the Heads of State and Government of the Member States, is a strong intergovernmental factor, due to the fact that the decision-making process for the relevant development steps of the Union is taken without the President of the Commission and the President of the European Council. The Council embodies this even more since here, next to the Parliament, the second Legislative Assembly consists only of Ministers of the Member States.

And third, there are parts which could be best analyzed by the theory of Neo-functionalism. The European Union is equipped with greater participation possibilities, which was a great goal of the Constitutional Convent. The European Citizens Initiative, the election of the European Parliament, and the consideration of the election result in the appointment of the President of the Commission have given new possibilities to the existing participation. For this proximity to the citizen was improved too. Also in the point of international agreements the competences lie with institutions of the European Union with binding decisions for the Member States. This is easily shown in Fig. 1.

It is now clear that the key points of the European Union, such as the right, the competences, the institutions, the foreign policy, and the areas of security, cannot be clearly confirmed neither by the Liberal Intergovernmentalism nor the Neo-functionalism. The attempt to describe the process of the Constitutional Convention up to the conclusion of the Treaty of Lisbon with its provisions either with one or the other theory works only when certain areas that speak for the theory are highlighted and others are blurred. Furthermore, certain developments and processes cannot be explained by either the Liberal Intergovernmentalism or the Neo-functionalism. The analysis has shown that none of the two hypotheses has neither been confirmed nor refuted. If the integration process cannot be answered clearly by the theories of Neo-functionalism or Liberal Intergovernmentalism, it will maybe be a good point to refine, further develop, or completely rethink the theories. This will be part of the next chapter.

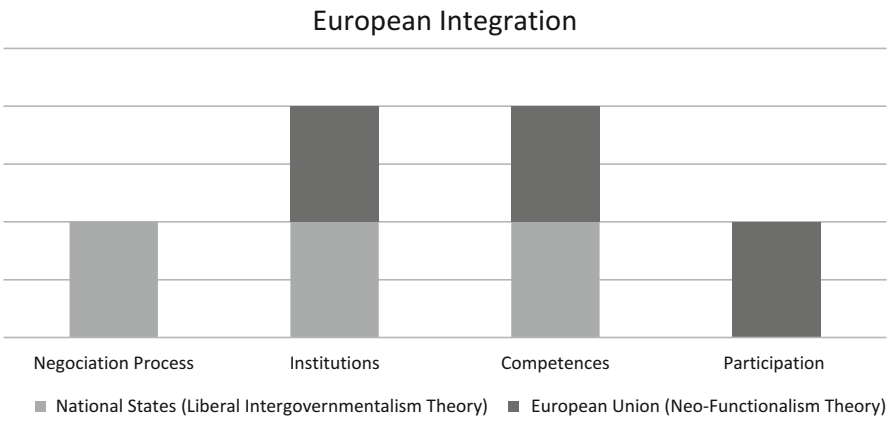


Fig. 1 European Integration (Source: Author's own conceptualization)

The New Theories of Integration and the Future of European Integration

There are a lot of new theories, which try to explain the process of European Integration. Two of them are especially interesting because they are redeveloped ones from the analysis above: The New Intergovernmentalism and the Postfunctionalism.

New Intergovernmentalism

The New Intergovernmentalism is a theory which considers the post Maastricht Treaty period after 1992. This time was marked by transition from a single market to a monetary union and expansion from 15 to 28 Member States, but also by the National States which take the main act in the integration process instead of supranational institutions like the European Commission and the Court. Domestic policy in negotiations of the Member States is preferred and the only move of power to a supranational level is if they are tended to entail the creation of "de novo" bodies. The theory also includes the hypothesis about the importance of deliberation and consensus building reflect, which is a decentralized character of decision building. The supranational institutions are far from resisting decentralized modes of decision building and policy making. The Commission makes no efforts and the Parliament restrains (Bickerton et al. 2015).

An interesting point is the fact that the theory addresses a change in national policy making. The elected People's Representatives are not the only decision-makers, but also informal meetings play an important role. In the European Council, bargaining and negotiations are adopted according to the classical, intergovernmental principle. But according to this analysis there is no normative, polity point on this.

It is more about policy and politics. Also the competences which are normative by institutions of the European Union cannot be described by the New Intergovernmentalism.

Postfunctionalism

Also for Postfunctionalists the era after the Maastricht treaty is a time of change in the process of European Integration. The relationship between identity and efficiency is the crucial point. Domestic policy connected with party competition, elections, and referendums are in focus. The integration achieved room for a Eurosceptic public. European issues have been started to be addressed and further fueled the party competition. This theory claims that identity and economic interest underlies preferences. On the one hand, identity becomes a stronger argument after Maastricht. On the other hand, the European Union wants to conclude targeted and progressive trade deals with like-minded partners. There is the desire that national and regional parliaments will not block the process of ratification. Hooghe and Marks proclaim in the Postfunctionalist theory that since there is a public debate on the European Union the national identity is in the focus. The identity is affected by consequences of a system of multilevel governance. Being a loser of globalization, national boundaries break down, immigration increase, and change in national sovereignty create sorrows and fears. Political parties want to win elections and implement their programs (Hooghe and Marks 2008).

The main point about the relationship between Identity and Efficiency is a possible good starting point to analyze how more integration could be achieved. This will be a good way to find possible ways to influence future decisions on European integration.

The White Paper

In 2017, the European Union celebrates its 60th anniversary. It is only conditionally a reason to celebrate. The analysis has already shown that the Treaty of Lisbon in some parts has more integration elements but there are also stagnating parts. The period after 2007 has passed through crises and unification problems. Increasingly intergovernmental solutions, especially in the refugee crisis and the planned first phase-out of a Member State, are a major cause of concern for visionaries of a United Europe. The domestic policy and protectionist ideas are increasingly favorable. It seems obvious that the European Union needs a new vision and strategies to be as successful and consistent as possible. On the 1st March 2017, Jean Claude Junker, the President of the European Commission, presented a reflection and a possible upcoming scenario: "The White Paper on the Future of Europe" (European Commission 2017).

The paper contains the drivers of change in the coming years and a number of scenarios as Europe might look in 2025. Also, the creation of a European defense

Union in full complementarity with NATO will be created. So, there will not be just a Neo-functionalism integration but more to federalism governance system.

Scenario two is the strongest intergovernmental and less neo-functionalistic model of all. As the only cooperation in Europe, the single market should survive. Parts like the security and migration policy will be ruled just bilaterally and with no single policy in Europe. Also in foreign and defense issues the National States will decide how and with whom they want to cooperate. The decision-making process between the Member States might be easier but the capacity for collectively acts are strongly limited. This scenario should also be seen as very unrealistic. At the moment, even the Eurosceptic movements have no interest in keeping the single market as the only supranational cooperation.

Scenario one and four are close in some points. The European Commission tries to shift more competences to the European institutions. There should be more cooperation in the management of an asylum system and integration. In security policy, the external border control should have stepped up gradually. Another progress will be a common foreign policy when the European Union speaks with one voice. Scenario four makes also the point that parts in which more integration is required are the single market, counterterrorism but also foreign policy and the creation of a European defense Union. In contrast parts like regional development, public health, standards of consumer protection, and parts of employment and social policy will not be directly controlled. Environment and safety at work will move to a minimum of collaboration. Scenario one mentions that National States and regional parliaments should not block and lengthen the process of trade deals with economic partner states. Both scenarios are propagating the hope for another spillover effect. Both scenarios can be good declared with the Neo-functionalist theory.

Scenario three has similar neo-functional features as scenario one and four, e.g., cooperation in the policies of managing asylum and integration system, external border control, foreign policy, and better military coordination, with the significant difference that member states participations are based on voluntariness. This is an interesting point, because maybe the stronger Member States could unleash a new integration process, by influencing the smaller ones, because of their interdependencies.

Conclusion

The causal analysis showed that there is no clear result for answering the research questions. The current state of European Integration after the last major treaty could not be adequately described with the used theories. The hypotheses were verified and falsified in certain areas. Processes of European Integration that affect a change in the existing norms and contracts are too complex to explain them by only one of the two most widely used integration theories. There are competencies in the European treaties, which are among supranational organizations and others which are among the National States. The integration theories may be more suitable for a politics analysis. The forms of the enforcement of interests, the carrying out of conflicts or

political action in the proper sense, and the struggle for gaining or maintaining power may be better understood with the existing theories of integration.

But how could we relate a reflection of the existing theories to Cyber Development? The White Paper of the European Commission offers on the one hand possible future scenarios, which could be good described by a theory; however, those are the most unrealistic ones (scenario two and five). On the other hand, the more probable scenarios one, three, and four are also mixed forms according to the theories. With the new theories of European Integration like the Postfunctionalism, new perspectives would be opened, like the individual preferences. Identity and efficiency influences the domestic policy of the Member States. The resulting output determines how topics are politicized. Politicization is one keyword of the System of Differentiated Integration by Frank Schimmelfennig, Dirk Leuffen, and Berthold Rittberger. Differentiated integration is not seen as temporary, but as an enduring characteristic of European Integration. For a better understanding, some key facts must be explained. There is a distinction between vertical differentiation, which explains the grade of centralization of policy areas and a horizontal differentiation relates to the territorial dimension of integration or how many member states participate. The main factors of integration are interdependence as the driver and politicization as the obstacle. *"We submit that the interaction of interdependence and politicization explains the general pattern of integration and differentiation in the EU. We conceive interdependence as the primary driver of integration. Interdependence creates the initial demand for integration, and a subsequent increase in exogenous or endogenous interdependence produces demand for more integration"* (Schimmelfennig et al. 2015).

The European Union as a System of Differentiated Integration is maybe the best tool to analyze the European future scenarios. This is because Inputs and Outputs can be measured in the process of integration. In cases where there is no interdependence, it does not matter if there is politicization. According to the European White Paper and the future of Europe, only cases with interdependence will have the chance for success. For Schimmelfennig, Leuffen, and Rittberger, the single market is something with high interdependence. It was the main project for the European Integration according to the Community method. The European single market has always been uniformly valid. There are low autonomy and identity costs for the Member states with the result of low politicization. Maybe the single market is the greatest sector of interdependence. All scenarios want to keep it and it is not questioned. Some scenarios want to implement a common foreign policy and military cooperation, differently pronounced. This policy fields have low independence and on the other hand a high grade of politicization. For this constellation, low integration is granted. The European Commission should focus on parts where interdependence can be raised and politicization stands low, or is in a positive view. For the future of European Integration and the development of Knowledge Society, there is a need for consideration of numerous relevant factors that may exercise an influence on politicization, especially individual ones like personal efficiency and identity from the postfunctionalistic view on the one hand and the grade of interdependence on the other hand (see Fig. 2). When there is need for more

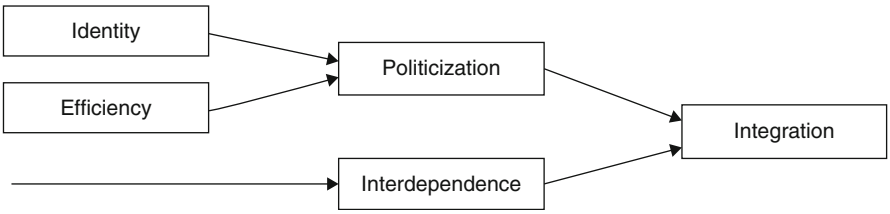


Fig. 2 European Integration in Cyber Development (Source: Author's own conceptualization)

integration, because of interdependence, there then should also be considered whether the individual priorities of the people of Europe support this. For the future in a Cyber Society and Cyber Economy, the European Union should focus on problems which could only be solved by a strong unified community. Like Jean-Claude Juncker already said on 16th December 2014: *"(. . ..) That is why we committed to driving change and to leading an EU that is bigger and more ambitious on big things, and smaller and more modest on small things"* (European Commission 2014).

Cross-References

- ▶ Academic Firm in Cyber-Development: The New Design and Redesign Proposition for Entrepreneurship in the Innovation-Driven Knowledge Economy
- ▶ Citizenship Education and New Media: Opportunities and Challenges
- ▶ Epistemic Governance and Epistemic Innovation Policy in Higher Education for Cyber-Development
- ▶ Quadruple and Quintuple Helix Innovation Systems and Mode 3 Knowledge Production

References

Bickerton, C. J., Hodson, D., & Puetter, U. (2015). The new Intergovernmentalism: European integration in the post-Maastricht era. *Journal of Common Market Studies, 53*(4), 703–722.

Bieling, H.-J., & Lerch, M. (2012). *Theorien der europäischen Integration*. Wiesbaden: Springer.

Carayannis, E. G., Campbell, D. F. J., & Efthymiopoulos, M. P. (2014). *Cyber-development, cyber-democracy and cyber-defense; Challenges, opportunities and implications for theory, policy and practice*. New York: Springer.

Clemens, G., Reinfeldt, A., & Wille, G. (2008). *Geschichte der europäischen Integration: Ein Lehrbuch*. Stuttgart: UTB.

Consolidated version of the TEU (Treaty on European Union). (2017). Eur-lex, Access to European law. http://eur-lex.europa.eu/.

Consolidated version of the TFEU (Treaty on the Functioning of the European Union). (2017). Eur-lex, Access to European law. http://eur-lex.europa.eu/.

European Commission. (2014). Press release (16 Dec 2014). Strasbourg. http://europa.eu/rapid/press-release_IP-14-2703_en.htm.

European Commission. (2017). White paper on the future of Europe. https://ec.europa.eu/commission/sites/beta-political/files/white_paper_on_the_future_of_europe_en.pdf.

Haas, E. (1958). *The uniting of Europe: Political, social, and economic forces*. Stanford: Stanford University Press.

Hellmann, V. (2009). *Der Vertrag von Lissabon: Vom Verfassungsvertrag zur Änderung der bestehenden Verträge – Einführung mit Synopse und Übersichten*. Heidelberg: Springer.

Hoffmann, S. (1964). The European process at Atlantic Crosspurposes. *Journal of Common Market Studies, 3*(2), 85–101.

Hoffmann, S. (1966). Obstinate or obsolete? The fate of the nation-state and the case of Western Europe. *Daedalus, 95*(3), 862–915.

Hooghe, L., & Marks, G. (1996). European integration from the 1980s: State centric v. Multi-level governance. *Journal of Common Market Studies, 34*(3), 341–378.

Hooghe, L., & Marks, G. (2008). A Postfunctionalist theory of European integration: From permissive consensus to constraining Dissensus. *British Journal of Political Science, 39*(1), 1–23. Cambridge University Press.

Knodt, M., & Corcaci, A. (2012). *Europäische Integration: Anleitung zur theoriegeleiteten Analyse*. München: UVK.

Mitrany, D. (1944). *A working peace system: An argument for the functional development of international organization*. London: Royal Institute of International Affairs.

Moravcsik, A. (1998). *The Choice for Europe. Social Purpose and State Power from Messina to Maastricht*. Ithaca: Cornell University Press.

Schimmelfennig, F., Leuffen, D., & Rittberger, B. (2015). The European Union as a system of differentiated integration: Interdependence, politicization and differentiation. *Journal of European Public Policy, 22*(6), 764–782.

Reviewing European Astropolitics

9

Boris S. Manov

Contents

Abstract

Since the Renaissance, Europe has been one of the foremost pioneers in political, scientific, and technological development. The creation and implementation of a common space policy within the EU will be vital in the new century. Hitherto countries within the Union have approached space in a diverse manner. Space is becoming gradually an important strategic sector and will be essential to the European strategic independence. This analysis will investigate, how Europe has approached space and cyber development, as well as analyze future implications and prospects. Moreover, we will look at the possible improvements discussed to make the EU more competitive and challenging in the traditional space powers.

Keywords

Cyber development · Space development · Space policy · Space technology · Cyber democracy · Europe · Astropolitics

B. S. Manov (✉)
Political Science, Researcher at University of Vienna, Vienna, Austria

Sofia, Bulgaria
e-mail: boris_manov@hotmail.com

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_64

Introduction

In the last 40 years, the nations of Europe have dwelled upon the idea of using space for civilian, commercial, and military purposes. However only recently have they began to elaborate on how should they approach space and cyber development. Although the European Space Agency (ESA) was created back in 1975, the members of the EU (European Union) did not commit to a common space policy until the 22nd of May 2007. As per the statement of ESA "Through this document, the EU, ESA and its Member States all commit to increasing coordination of their activities and programmes and to organizing their respective roles relating to space" (IBP 2013: 32). Despite those statements, almost 10 years later, we still have not seen the required commitment to improving the common space policy, due to a set of reasons beyond the control of the EU institutions. The two discourses, supranationalism and intergovernmentalism, have fostered some success in developing the common *European astropolitics*, nevertheless, space and cyber development remain exclusively in the national sphere of management. Furthermore, as the two fields of development require large investments and extensive technology, not all members, who have signed the common space policy, have wholeheartedly committed to participating in this endeavor. If the EU is to become truly a global competitor among traditional spacefaring nations, there are a set of objectives in astropolitics that need to be agreed upon and fulfilled, before challenging the USA, Russia, and China economically, technologically, and socially regarding space. This analysis will review the political developments between space actors on supranational, intergovernmental, and national level. In addition to that, we will look at the financial commitment of the member states in the recent years and the current figures indicating the interest in space. Additionally, we will assess the technological advancements and companies involved in the EU space industry. To conclude this analysis, I will mention future implications and already proposed measures that the EU can undertake to improve their space and cyber development.

Politics behind Astropolitics

The first part of the analysis will review the policies, strategies, activities, and political programs undertaken so far by the relevant actors in the European space domain. Space and cyber policy development for Europe have been ongoing ever since the creation of the intergovernmental institution, the European Space Agency. ESA is a clear example where intergovernmentalism has been pivotal in the development and execution of space tasks by bringing together the different nations of Europe in the strategic space sector. ESA has been essential in coordinating all space activities and missions conducted by Europe. The European Space Agency essentially works by the combined efforts of the countries participating in ESA's governing Council: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, The Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, and the UK. ESA

has three types of activity: basic, inspirational, and utilitarian. "The 'Basic' space includes all the programs, capabilities, and requirements necessary to guarantee strategic independence in the space realm. This includes guaranteed access to space and guaranteed use of space. Capabilities and requirements include maintaining Europe's industrial and technological capabilities so an independent space program can exist. 'Inspirational' space activities involve science and exploration. This type lends itself to endeavors involving international cooperation. The International Space Station is a good example. The third type, 'Utilitarian', includes public or private space based services, such as telecommunications, navigation, Earth observation, and weather satellites". Next through the supranational body of the European Commission, proposals and drafts are put forward to develop a common space policy. The EC takes the active part in developing the right framework for EU space usage. In the 2003 White Papers, the European Commission pointed out to the two dangers regarding space: the decline of the leading space companies and the decline of space power capabilities (Gleason 2006: 17). The two matters are being addressed in every new proposal for space policy. Within the EC, several DGs are included in the policy creation, with DG Growth being the most prominent of them. While EC conducts the political side, ESA runs the technological aspect and helps EC to implement and execute objectives and goals. The European Parliament, another supranational body, also expresses a positive attitude toward a common space policy development for a long time. The fact that this new economy and technology will be based on space development will also make Europe more competitive and autonomous on the international scene as well as give the people of Europe more jobs and space-based expanding economy. In the words of Gleason, "The European level is positioning itself to be the most important level, envisioning an entirely new economy of scale and enabling a qualitative leap forward in European space power capability" (Gleason 2006: 9).

Thus, important space policy needs to pass three different levels: *supranational*, the European Commission; *intergovernmental*, the European Space Agency; and *national*, the member states, respectively, with their own space programs. Ultimately though, implementing the final decisions will be in the hands of the national governments. In vision of that, Nicolas Peter further outlines: "Europe, through various institutions, now officially recognizes space as a strategic asset and views space as a tool for maintaining Europe's political and economic strength and for the implementation of EU goals" (Peter 2005: 293). Recognizing these benefits, the EU is moving toward creating a zone of interest in space. Moreover late in 2003, ESA redefined the meaning of "peaceful purposes" in its charter to mean "nonaggressive," rather than its traditional definition of strictly non-security, non-defense, and nonmilitary related, highlighting Europe's soft power approach (Gleason 2006: 15).

Yet, a common space policy has a lot to do with the security policy of the various member states. To coordinate and enhance their security services, the EC decided to implement the Space Situational Awareness (SSA) programme, to provide data and information regarding the space environment (McCormick 2015: 43). The SSA program has three main activities, which are Space Weather (SWE), Near-Earth Objects (NEO), and Space surveillance and tracking (SST). SWE serves to ". . . to

support Europe's independent utilization of, and access to, space through the provision of timely and accurate information regarding the space environment, and particularly regarding hazards to infrastructure in orbit and on the ground" (ESA SSA 2018a). The NEO "provides warnings on potential asteroid impact hazards including discovery identification, orbit prediction and civil alert capabilities" (ESA 2017b). The SST monitors the space debris in space and helps satellites remain operational, by warning of dangers and avoiding them (ESA SSA 2018b). The GOVSATCOM is the third pillar for the current EU space security development which "aims to pool and share governmental and commercial satellite services to provide secure and guaranteed access to SATCOM for a wide range of governmental applications" (ESA 2017c).

Peter also shows how common space security policy directly relates to the security policy on a supranational level: "It can give Europe the full capability to act independently in conflict prevention and crisis management tasks to support its Common Foreign and Security Policy (CFSP) and the European Security and Defense Policy (ESDP)" (Peter 2005: 266). This could also serve as an active tool for delivering the Petersberg tasks and ensuring the supranational security of the continent. Yet, since space has such an impact upon the society, any final decisions taken in regard to space security again lie exclusively in the hands of the national governments. Hence EC and ESA can only serve as guidance, on how the states of Europe can combine their efforts to create a more efficient and competitive space framework. The signing of the European Guaranteed Access to Space (EGAS) in May 2003 displayed a great political will of the European space actors to improve their access and coordination in space. Moreover, in late 2004, those same actors across Europe gathered for the first European Space Council meeting. The Council aims to coordinate and facilitate cooperative activities between the European Community and ESA (EC 2004). The Framework Agreement was signed at the Fourth Space Council in 2007; it started serving as the basis for developing solution on European Space Policy. In the resolution the EC and ESA recognized the economic limitations of space programs and proposed a collective program, to be able to coordinate space activities, to act more efficiently, and to remove any duplicities (McCormick 2015: 55). Next in the treaty of Lisbon of 2009, under Article 189, the EU gained the new power to create an autonomous space program. That would become a common policy, which can be established within the EU as a Common European Space Policy (CESP), within the institutional framework of the union.

In addition to these agreements, there are several programs, which the European Union is running as joint initiatives: Galileo, Copernicus, and the Global Earth Observation System of Systems (GEOSS). In addition to these main three programs, ESA is operating a number of missions single-handedly and jointly with other countries such as Japan, China, and USA. Some of them are the Rosetta probe module, the Gaia space observatory, and the collaboration NASA-ESA, the Solar and Heliospheric Observatory (SOHO). Such scientific and operational programs serve Europe in all spheres: independent access and control of space, communication, intelligence, navigation, positioning, HD imagery, meteorology, and even missile launch early warning. These space applications would allow Europe to

possess the capacity of cooperating and competing on the geopolitical map with other traditional space powers while enhancing socially the whole continent. Nonetheless, those initiatives are expensive projects that first need to be agreed upon and then also financed. In the words of Gleason, "Commitment of money is often considered the ultimate demonstration of political will".

Financial Commitments to the Space and Cyber Development

Financing the space strategical access is an expensive venture. Few countries have such resources and even fewer have space programs in place. Europe needs to cooperate and co-finance joint programs, to initiate space and cyber development. There are several discourses, which have looked at individual financial participation by space actors in Europe. In a recent analysis in 2013, Machay and Pochyla took space policy and converted it to a common good, desired by the different nations. According to them the ". . . Income elasticity helps us to understand how a consumer perceives goods, depending on changes in his or her income – or one can say in changes of total expenditures. Thus 'a demanded quantity of space policy', cannot be really measured, but the finances allocated from the total budget of a nation, can give a fair idea of how interested a government is in developing their space sector." The two scholars actually reviewed absolute vs. relative spending of the member states. To be able to look at financial commitment over time allows the identification of economic dedication to space development. However, "only a positive or a negative value is not a sufficient indicator of how the country perceives space policy as its own priority. For them it is necessary to interpret the sign in the context of the development of the government expenditures in a given year" (Machay and Pochylá 2013: 208). Setting concrete variables for the analysis of the data, Machay and Pochyla identified three groups of nations and grouped them by their financial commitment to furthering space initiatives. These three groups are split into activist, active, and passive actors.

Under the first group, the *activists*, the government is perceiving the expenditures on space exploration and exploitation as a top priority. This implies that the government expenditure on space grows faster than the total expenditures. It also means that when the total government expenditure is decreased – the government reduces the expenditures, but the spending on space (policy) either stays the same or continues rising. In the second group of actors, the *actives* are also interested in funding their space programs; however they tend to concentrate on long-term space strategies, as they aim to minimize the variations in funding space policy. Political and economic factors do play a role in determining the fiscal support, but the persisting goal of pursuing space remains the long-term objective, and there is a constant economic support. In the last group, under *passive* policy, countries view other policies as more important and actually the spending on space decreases, not only in absolute numbers but also as a relative value (Machay and Pochylá 2013: 210). According to the results from their research, the top activist countries are Denmark, Germany, Norway, Portugal, and Austria. Countries such as Finland,

Ireland, and Slovakia have pursued constancy in space development. Surprisingly, traditionally interested space actors such as France and Italy have found themselves in this group. Decreases in relative spending toward the space strategic sector have been caused by fiscal deficit and political concerns. In their conclusion, Machay and Pochyla stated: "Overall, there is not a strong long-term devotion toward activities in space. We see that the budgets allocated to space exploration and exploitation do not show clear continuity in spending and that they evolve more or less randomly in time, where funding significantly fluctuates" (Machay and Pochylá 2013: 215).

Patricia McCormick supports these findings, by presenting a more recent analysis of financial commitment to one of the joint programs, the SSA Preparatory Program. For the period between 2013 and 2016, the initial €300 million budget proposal was revised to €100 million and then cut back to €46.5 million (McCormick 2015: 48). Decrease of the political will is evident with such figures. In spite of that in the recent Space council meeting in January 2018, the foreign minister of the EU, Federica Mogherini, stated that Europe has the second biggest space budget in the world (ProductiehuisEU 2018). The Galileo program alone costs €3 billion to develop and maintain. The Copernicus program, the largest Earth observation program, is estimated to cost €4.3 billion between 2014 and 2020. The communication and navigations ground system, EGNOS, will cost the EU €2.7 billion for the same period (IG 2012). As far as the budget of ESA is being concerned for 2018, it has been decided to be €5.6 billion. This number is divided by mandatory and optional funding. The mandatory is based on the countries yearly GDP, and the optional is for members that are interested (ESA 2018a).

In order to maintain such high numbers, there have been numerous calls on to the private sector, to participate more actively in space development. According to the EC "(Space industry) . . . It drives scientific progress and boosts growth and employment in other areas such as telecommunications, navigation, and Earth observation" (EC 2018). Moreover, Mogherini has stated during the last EU's Space Council meeting that the space industry of Europe is unique, in such that a mix of small, medium, and large enterprises guarantees the quality and innovation. Likewise, the industry needs certainty about resources and long-term strategy. The EU institutions further the interest of the industry in many nations across the globe, by creating bilateral agreements and using economic diplomacy (ProductiehuisEU 2018). Furthermore, the private sector has been essential for Europe to benefit socially and economically as well as remain competitive and innovative in the space technology sector.

EU Space Technology

The third part of this research reviews the technological side of space development in Europe. The first instance, where the EU provided a significant boost for the European-level of space, was with the Constitutional Treaty for Europe signed in 2004, including space as a priority. The foremost European political leaders back then accepted the notion that Europe's autonomous access to space, and its space

power capability, would be a vital European strategic asset. From that stems the European Space Program, which determines the priorities, objectives, budgets, roles, and responsibilities, and it will include R&D, infrastructure, service, and technology. This mode of thinking and political will becomes beneficial for the space industry of Europe, as it provides funding and direction for innovative and cutting-edge technology (Gleason 2006: 20).

Traditionally, Europe expresses competitiveness in the spheres of engineering, physics, mathematics, and chemistry. Being a leader in these fields surely has allowed Europe to also challenge traditional space powers, but to remain here on top, the EU has had a need to innovate in the space sector and space technology production. In an elaborate paper, published back in 2005, Nicolas Peter discussed in lengths the technological progress in Europe toward developing space technology and the needed capability to compete in the global realm. Concurring with Peter, "The first real space initiatives for the EU, through the European Commission, were in the application program for global navigation satellite system Galileo and the operational Earth observation system for Global Monitoring for Environment and Security program (GMES)" (Peter 2005: 272).

Galileo is the equivalent of the US's GPS. The first of the launches to set the Galileo constellation of satellites took place in 2011, with the launch of the GIOVE-A. Currently, Galileo consists of 22 satellites, and additional four satellites are being planned to be launched by the end of 2018. By the end of the system deployment, there should be in total 30 satellites, to be positioned in the medium Earth orbit at 23,222 km above the Earth's surface. The system is designed and intended to become fully operational by 2020 (ESA 2017a). The system serves five purposes: open-access navigation, commercial navigation, search and rescue, safety of life navigation, and public regulated navigation (ESA 2010). The EGNOS program is a geostationary navigation system, composed of over 40 positioning stations and 4 main control centers, supporting the Galileo satellite program (ESA 2013). To possess such a navigational system allows the space actors within Europe to coordinate better and to be more autonomous in space sectors.

Besides Galileo and EGNOS, the European Commission and ESA have run a third program, Copernicus, previously known as GMES. The Copernicus observation program serves to monitor, track, and relay data for social, economic, and military purposes. Currently, ESA has five missions under the Sentinel program in an active status: radar and super-spectral imaging for land, ocean, and atmospheric monitoring. Each of the missions requires two satellites, and currently there are five Sentinels gathering data. Up to another ten have been planned for launches in the next 3 years. The developer of the Sentinels is Airbus Space and Defense. The European Aeronautics Defense and Space Company (EADS) was a corporation composed of Airbus Military, Astrium, and Cassidian, leading to recent mergers, and was rebranded, in 2017, only as Airbus (Parker 2014).

The different divisions of Airbus provide sensors, radars, satellites, and other space technology for the European space actors. Besides Airbus, there are several other space industry companies worth mentioning. The Arianespace, founded in 1980, manufactures launch vehicle. It has launched 550 satellites in the last 38 years,

in collaboration with CNES, from Kourou. Arianespace has developed different types of rockets for the different tonnage of the payloads. The smallest one, the solid-fueled Vega, carries up to 1,450 kg of payload. The technology for the medium-sized soviet Soyuz was bought from Roscosmos, for manned missions up to 4,400 kg. The Ariane rocket, the heaviest of the three, can carry up to 21,000 kg and is used mainly for missions in the geosynchronous orbit or beyond. As of January 2018, Arianespace has signed contracts for the development of Ariane 5 ECA launches up until 2022, after the planned introduction of Ariane 6 in 2020 (Caleb 2018). Boasting with five versions of the Ariane rockets, Arianespace has dominated the space market for a long time. Nonetheless, with the arrival of the new reusable Falcon 9 rocket by SpaceX, the Europeans have taken a step back.

The different rockets that are being used are referring to several rocket launch facilities that the nations of Europe are utilizing, but the main one is the Guiana Space Centre (GSC), located in Kourou, French Guiana. The facility began operating back in 1964, under the French Space Agency (CNES). In 1975, CNES joined forces with ESA and have ever since maintained and funded the spaceport. The location is perfect, as it allows for launches to the different orbits of the Earth, and there are no earthquakes or hurricanes, which can endanger the launch facility. Additionally to GSC, there are several other rocket launch sites, but due to their limited size, they have been only smaller rocket test sites for European space actors.

In general, the European countries, agencies, and companies need to operate with immense amount of resources, to allow the EU to remain relevant in the space sector. To bring down expenses, national and international cooperation and sharing of technology as well as multilateral agreements have been instrumental for Europe to become the number two space power in the world currently. More specifically, the cooperation with the USA and Russia has aided in the exchange of technology and data. For example, the EU-US satellite data arrangement has helped to monitor and map Hurricane Harvey back in 2017. Also the collaboration between ESA and Roscosmos, with the launch of Soyuz from Kourou, was a milestone in the strategic cooperation between EU and Russia (ESA 2018b). But to become fully autonomous with regard to space, the EU needs to fully commit itself to advancing their space development efforts. That can only happen, when the supranational bodies of Europe propose mandatory and concrete measures for all members (member states) of the EU, to accept and to be implemented. This includes to involve the private sector and to make the market more competitive with reference to space technology, which would allow for significant improvements and diminishing costs in space and cyber development.

Implications/Improvements

In the last part of our analysis, we will discuss the possible implications for enhancing the common space policy of the European actors. As mentioned in the first part, the political will of committing oneself to a common space policy is variable. The EC, ESA, and the member states have all proposed different

legislations, which would in general boost the EU space. However, since different matters are pending for the different nations, financial stimulus has declined. Developing the space and cyber sector remains a complicated subject, as the costs are high, and the interest in devoting these resources is diverse between the EU members. In 2016, during a joint conference of US and European space representatives, the deputy director of the DG Growth, Mr. Pierre Delsaux, expressed the need for how the space strategy should be inclusive and should involve ESA, the EC, and the member states, and industry should be included as well. In his opening speech, Mr. Delsaux mentioned four important messages to be relayed forward: a long-term space strategy for Europe, bringing space down to Earth, promoting innovation and competitiveness, and protecting space assets. The long-term strategy is apropos the synchronization and implementation of space policy across all the European actors, from supranational down to national levels. Consenting to Delsaux', the inclusiveness remains the most important feature for establishing the strategy. Bringing space down to Earth would explain to the ordinary citizens why space is so important, how space can help the economy, and how should we create growth with space. Innovation and competition refer to creating new ways of how technology should function and how to invite more private investors. Helping the start-ups and continuing the support for Galileo and Copernicus also shows commitment from the institutions on a political level. The last message of the deputy is the need for protection of the space assets, which clearly refers to the issue of SSA and GOVSATCOMs (EU in the USA 2016). The EC states on their website: "In a context of increased security threats, there is a growing need for secured satellite communications (SATCOM) to support institutional users in the execution of security missions and the protection of critical information infrastructure" (EC 2017). The limited availability of these services to some countries persists, and implementation is still pending.

However, once completed, this would serve vital to civilian and military objectives. Additionally, the EC adopted at supranational level a European Defense Action Plan – a plan to develop the defense industry of Europe. If member states do need capabilities in the future, they would also need the industry to develop this capability. Additionally, the European Defense Fund was setup to support defense and R&D in the European defense sector (EEAS 2017).

During the last Space Council, Mogherini announced a global strategy, accepted by all European actors, "To promote autonomy and security of our space-based services." The strategy outlines the importance of a common space program for cooperation, common governance, security, and economy (EEAS 2018). Such words, from the EU's foreign minister, display adequacy from the union in dealing with the new space and cyber reality. Looking after Europe's interests as a whole at first and then making sure that the continent is united, this can only ensure space progress. In the current age of world political turmoil, economic competitiveness and a decline in quality of social life, the next most important strategic sector for development will be space. If Europe wishes to remain geopolitically, economically, and militarily competitive, they need to pool more resources into R&D for space technology and to collectively agree upon harmonizing the space framework behind it. Additionally, using the traditional soft power skills, the EU should continue to

promote cooperation and joint projects with non-EU agencies. Perhaps, a creation of a new DG, which deals solely with space, will display even bigger political will for such a goal. All in all, in any way that the EU continues, it will greatly impact the future of Europe for better or for worse.

Conclusion

Space and cyber development will be vital in the near future. This analysis has moved mainly through the space development of the EU. The cyber development is intertwined with space and vice versa. The two go hand in hand, as anything that consists of space technology, will have cyber elements behind it. Also in any way that cyber develops, it is most natural to expand into space, as the next most important strategic sector. Any human space expansion will have the cyber element. Both sectors of development would allow the different space actors to innovate, compete, and cooperate to further their gains on the global scene. *This review of the European astropolitics* has glanced briefly the historical and current state of European space, as well as the connected cyber development. It has also reinforced some suggestions about the future. *In the end, space and cyber development will be inevitable for Europe*.

Cross-References

► Space Defense: A New Offensive

References

Caleb, H. (2018). Arianne 5 down to two dozen launches before Ariane 6 takes over. Retrieved on 3 Mar 2018 from http://spacenews.com/ariane-5-down-to-two-dozen-launches-before-ariane-6-takes-over/.

EC. (2004). First ever 'Space Council' paves the way for a European space programme. Retrieved on 3 Mar 2018 from http://europa.eu/rapid/press-release_IP-04-1406_en.htm.

EC. (2017). Space and Security: GOVSATCOMS. Retrieved on 3 Mar 2018 from https://ec.europa.eu/growth/sectors/space/security_en.

EC. (2018). The space industry. Retrieved on 3 Mar 2018 from http://ec.europa.eu/growth/sectors/space/industry_en.

EEAS. (2017). Launching the European defense fund. Retrieved on 5 Mar 2018 from https://eeas.europa.eu/sites/eeas/files/launching_the_european_defence_fund.pdf.

EEAS. (2018). Federica Mogherini's opening speech at the 9th European Space Council. Retrieved on 26 Feb 2018 from https://www.youtube.com/watch?v=Gy7bUnWrgww.

ESA. (2010). Galileo services. Retrieved on 3 Mar 2018 from http://www.esa.int/Our_Activities/Navigation/Galileo/Galileo_services.

ESA. (2013). EGNOS: Navigation. Retrieved on 3 Mar 2018 from http://www.esa.int/Our_Activities/Navigation/EGNOS/EGNOS_Open_Service_available_a_new_era_for_European_navigation_begins_today.

ESA. (2017a). What is Galileo? Retrieved on 3 Mar 2018 from http://www.esa.int/Our_Activities/Navigation/Galileo/What_is_Galileo.
ESA. (2017b). Near Earth Objects. Retrieved on 3 Mar 2018 from http://www.esa.int/Our_Activities/Operations/Space_Situational_Awareness/Near-Earth_Objects_-_NEO_Segment.
ESA. (2017c). GOVSATCOM. Retrieved on 1 Mar 2018 from https://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/Govsatcom_Precursor.
ESA. (2018a). ESA Budget for 2018. Retrieved on 1 March from http://www.esa.int/About_Us/Welcome_to_ESA/Funding.
ESA. (2018b). Soyuz. Retrieved on 3 Mar 2018 from https://www.esa.int/Our_Activities/Space_Transportation/Launch_vehicles/Soyuz.
ESA SSA. (2018a). Space weather. Retrieved on 3 Mar 2018 from http://swe.ssa.esa.int/ssa-space-weather-activities.
ESA SSA. (2018b). Space surveillance and tracking. Retrieved on 3 Mar 2018 from http://www.esa.int/Our_Activities/Operations/Space_Situational_Awareness/Space_Surveillance_and_Tracking_-_SST_Segment.
EU in the USA. (2016). EU-U.S. Space policy conference. Retrieved on 23Feb 2018 from https://www.youtube.com/watch?v=zFmMg3kkLkc.
Gleason, M. P. (2006). European Union space initiatives: The political will for increasing European space power. *Astropolitics: The International Journal of Space Politics & Policy, 4*(1), 7–41.
IBP. (2013). *European space policy and programs handbook* (p. 32). Washington, DC: International Business Publications.
IG [Inside GNSS]. (2012). EU's Galileo and EGNOS expect 2014–2020 Budget boost of $9.1 billion. Accessed on 3 Mar 2018 from http://www.insidegnss.com/node/3012.
Machay, M., & Pochylá, J. (2013). European attitudes toward space exploration and exploitation, astropolitics. *The International Journal of Space Politics & Policy, 11*(3), 203–217.
McCormick, P. (2015). Space situational awareness in europe: The fractures and the federative aspects of European space efforts, astropolitics. *The International Journal of Space Politics & Policy, 13*(1), 43–64.
Parker, A.. (2014). EADS changes name to Airbus. Retrieved on 25 Feb 2018 from https://www.ft.com/content/9e29cfb0-73be-11e3-a0c0-00144feabdc0.
Peter, N. (2005). Space and security: The emerging role of Europe. *Astropolitics: The International Journal of Space Politics & Policy, 3*(3), 265–296.
ProductiehuisEU. (2018). 'EU 10th conference on European space' – "More space for more Europe". Retrieved on 3 Mar 2018 from https://www.youtube.com/watch?v=uwKN-UcphFs.

Society in Need of Future: Complementary Foresight as a Method to Co-create Transition

10

Doris Wilhelmer

Contents

D. Wilhelmer (✉)
Center for Innovation Systems and Policy, AIT Austrian Institute of Technology GmbH, Vienna, Austria
e-mail: doris.wilhelmer@ait.ac.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_27

Abstract

The most effective way to manage change successfully is to create it! (Drucker PF, *Managing in the next society 1994*. New York: Publisher St. Martin's Griffin, 2003) Facing upcoming grand challenges policy coordination turns out to be a daunting task and yet can be promising even when facing difficult circumstances. New patterns of thinking and acting emerge beyond governmental steering efforts. The complementary foresight approach offers a multi-method coordination framework for detecting accessible as well as tacit knowledge of diverse stakeholders.

As a matter of principle future cannot be forecasted. The most effective way to foresee future is to jointly shape it! Complementary foresight offers a neutral room for transformation and co-creation room beyond distinct determination of future. In co-creation, stakeholders gain new insights into complex interdependencies of the system as a whole. Self-organized as if initiated by an invisible hand anticipated, desirable futures allow mutual learning and behavior in rehearsal for transition. This allows changing mind and actions before official regulations and instructions tell to do so.

Society is in need for desirable futures! Citizens and organizations coordinate themselves by means of internal images and stories. Past and futures are no realities but only grammatical principles of how to construct reality. Thus "future images" allow positive sense making by combining novel images with traditional stories. Today's crisis and disruptive changes require knowledge and joint, powerful, collective pictures serving self-confidence and self-responsibility of citizens engaged: They are the change in the present for the present allowing policy governance from future perspective.

Keywords

Grand challenges · Governmental coordination · Transformation, policy learning · Mutual learning · Context-governance · Transdisciplinarily · Participatory foresight · Complementary foresight · Multi-method coordination · Co-creation · Coproduction · (Trans-) organizational-development · Network governance · Constructivism · Knowledge democracy · Quality of democracy · Cyberdemocracy

Introduction

Today we face grand challenges to be answered in an adequate way by coordinated actions of policy makers, scientists, and managers of diverse industries:

With respect to climate change, figures show that temperature will increase in the southern and eastern European continental regions as well as in the regions near the Alps reaching up till 180 hot days per year and doubling hot days in Austria in 2070 (PLUREL project, EUROSTAT, Boitier et al., AIT). These trend lines will affect eastern cities where population is predicted to shrink up to 25%, and GDP per capita

is said to remain lowest in comparison to northwestern Europe. Facing the impacts of demographic change people in the age of 80+ will double in Europe until 2080, which in the case of Austria means that 25% of the population will be older than 64 years. When running for reelections short term oriented politicians often revival backward oriented, national policies instead of, e.g., utilizing today's flow of refugees for preventing from shrinking population and collapsing social systems.

The term "Grand Challenges" goes back to the European Horizon 2020 strategy addressing major concerns shared by citizens in Europe and elsewhere and aiming at solving key global health and development problems by agenda setting of policy priorities. Thereby issues like "health and demographic change, food security and water management, clean energy and green transport, climate action and resource efficiency, inclusive and secure societies of Europe and its citizens" were identified by the European Commission Priorities in the program of Horizon 2020.

On EU level this challenge-based approach brings together resources and knowledge across different nations, fields, technologies, and disciplines, including social sciences and the humanities for research and innovation related activities.

The issues covered by the term "Grand Challenges" are grand in scope and scale and are generally made up of "wicked problems" (Rittel and Weber 1973) that are difficult or even impossible to solve by single agencies or through rational planning approaches.

Grand Challenges Driving Change

The articulation of grand challenges is hardly novel and lies in the increasing attention given to such issues in formulating new missions for policies. However, these efforts face many practical and conceptual hurdles. Grand challenges are by nature complex and largely impervious to top-down rational planning approaches. Furthermore, any attempts to address them must span a number of long-standing organizational, epistemic, and sectoral boundaries (Cagnin et al. 2012).

Transformation is a systemic phenomenon by nature as it results from the continuing interaction between different actors and organizations (Freeman 1970). This means that an organization does not change in isolation but rather in interaction with its environment. Such environments are complex by nature and difficult, indeed, mostly impossible, to shape with a view to directing transformation in a predictable top-down manner. This has implications for any attempts at guiding transformation and innovation activities towards grand challenges.

This highlights the fact that a one-size-fits-all approach to promoting transformation is unlikely to work across the range of grand challenges to be addressed. Rather, a more nuanced and context-sensitive approach is required that takes into account the nature of each challenge and the industries and sectors that need to react and that will be affected. It is here that, e.g., innovation system failures that demand policy attention tend to be identified, focused around actors' capabilities, the scale and nature of system interactions, and the workings of institutions (Arnold 2004; Woolthuis et al. 2005).

Context-sensitive approaches aiming at transformation as well as innovation have to activate various resources. For successfully doing so (a) facilitation of experimentation and learning as safeguarding "variety," (b) nurture knowledge development besides science and technology, (c) knowledge diffusion, (d) guide actors in selecting options for investment, (e) create spaces for radical innovations and new markets by setting standards or regulations, (f) develop and mobilize human resources and financial capital (Cagnin et al. 2012).

Grand Challenges Indicating Coordination Potential

The special nature of the requirements of grand challenges to find effective solutions brings to the fore concepts such as transformative (in radically changing unsustainable current practices), responsible (going beyond profit and economic competitiveness to safeguard social and environmental goals), and social (for the public good) innovation (Depledge et al. 2010).

Grand challenges require *broader changes in human perceptions and behavior*, as well as social innovations promoting nontechnological solutions. The challenge is for business, governments, and societies to align and evolve into this new direction, identifying alternative solutions and moving away from the current state of affairs (Cagnin et al. 2012).

Starting with the *structural elements*, the global character of grand challenges and their boundary-spanning nature transcends both epistemic and administrative boundaries and implies a greater number and wider variety of actors involved in innovation systems (Cagnin et al. 2012).

Continuing with *soft institutions* (e.g., values) findings tell that changes here are critical in determining progress in finding viable paths for tackling grand challenges and for changes in paradigms that may entail. Finding a solution to the problem of scarce energy resources, e.g., requires not only surpassing long-established stakes in certain resources but also a change in behavior, norms, and values of societies (Cagnin et al. 2012). Other changes required in soft institutions concern the motivations and focus of business actors, since certain grand challenges call for social responsibility and greater orientation of business focus towards the public good. This change is reflected in terms such as corporate social responsibility, corporate citizenship, or stakeholder theory (Smith 2000).

A number of *actions* promote to systemic reorientation towards grand challenges such as engaging different voices, protecting spaces, balancing interests, making connections, coordinating experiments, and levering investments: There is a need for policies that are related to *networks, community building*, visions, experiments, and learning. Such sociotechnical approaches highlight co-evolution, multidimensionality, complexity, and multi-actor processes (Cagnin et al. 2008).

Clearly aiming at societal and institutional transformation Boden et al. (2010) highlight the need for the creation of more *transparent and accountable forms of governance* that are better able to anticipate and adapt to the future and thus address common challenges, and to spread democracy and transparency at the global level. In this regard, foresight as a forward-looking approach is a tool of governance allowing a promising role to play in reorienting social and innovation systems towards grand challenges.

Crucially, at least from the perspective of transcending boundaries to better address grand challenges, forward-looking approaches such as foresight bring *longer-term perspectives* and broader knowledge bases into decision-making processes. By doing so, they place greater emphasis on holistic and multiple perspective approaches under which many potential levers for shaping the direction of innovation can be identified.

From a policy arena perspective, this *coordination potentia*l can enhance communication and understanding between policy "silos" and thereby support the emergence of an effective policy mix for innovation. In this way forward looking processes can enable governments and other actors to become more adaptive and capable of enacting systemic change (Cagnin et al. 2012).

In Need of Future-Oriented, Governmental Coordination

In search of sustainable pathways for joint solutions, the coordination of various highly distinct organizations deriving from different sectors, disciplines, etc. is a must. This coordination featuring different functions and goals is complicated to begin with, since organizations draw their legitimation from serving their specific goals which may or may not be congruent with the goals of other involved organizations (Peters 2013).

Complications stem from the fact that organizations are varying with respect to norms, values, cultures, clientele, and practices developed to navigate the daily tasks specific to each organization (March and Olsen 1989; Hall and Taylor 1996; Wagenaar 2004). The uniqueness of this set of variables characteristic for an organization is an important reason for the failure of interorganizational communication, cooperation, and coordination and thus learning in politics.

In order to be able to grasp the unique type of foresight-learning processes, it previously is essential to shortly explain established forms of learning and transformation in politics.

Traditional Forms of Policy Learning

A number of classifications of learning in politics have been advanced during the last decades. P. Biegelbauer thereby distinguishes between five forms of learning (Biegelbauer 2015):

Instrumental Policy Learning

Instrumental policy learning is about the viability of policy instruments and implementation designs directed towards policy instruments. The instrumental learning applies to questions of instrument selection and development and thereby often is based on learning processes among ministries during selection processes.

Managerial Learning

As a term related to instrumental learning, managerial learning is concerned with policy delivery and the implementation of policy instruments (Schofield 2004). Thereby, it is about the way in which policy instruments are constantly interpreted,

adapted, and filled with new meaning in the practices of staff working on the implementation of policies (Freeman 2006).

Social Policy Learning

Social (policy) learning is oriented towards the goals of policies, their acceptability and practicality but also on mechanisms, theoretical underpinnings, and interpretations of the way in which policies aim at effecting their environment (Hall 1993). Oliver and Pemberton (2004) have shown that social learning is more evolutionary and involves more and lengthier struggles for the supremacy of policy ideas. Following Beland and Cox (2013) policy entrepreneurs often try to manipulate ideas, which form the basis for paradigm changes in process of social learning.

Reflexive Policy Learning

Reflexive learning focuses on the ways in which learning takes place, its rules and mechanisms (Bandelow 2009). For instance, policy actors become uneasy with the ways in which experiences lead to changes in policy-making and introduce new instruments or coordinate reflection processes differently, hereby changing the way of learning.

Political Learning

Political actors define policy targets in order to reach certain goals, to become reelected or obtain a certain political function, which they try to obtain among other things, by devising policies. Political learning can also be about strategies and procedures, that is, ways to influence political processes so that a policy can be deployed. Yet this form of learning again is about efforts to gain political posts and function.

Future-Oriented Policy Learning

Need of Reflexive Policy Learning

With increasing numbers of governmental but also nongovernmental organizations taking part in the governance of society, the coordination of diverse sets of organizations becomes more important. A large number of measures have been tried for enhancing government coordination (Peters 1998, 1996; Verhoest et al. 2007; Lindner 2012; Biegelbauer 2013; Laegreid et al. 2015) for both the policy and administrative levels.

Coordination moreover cannot be a goal in and by itself. It firstly serves the concrete goal of making governance more effective and efficient and, secondly, it comes with costs attached.

Recent literature emphasized the importance of a number of factors for achieving coordination such as the perception of the necessity of coordination, an appropriate sharing of costs and benefits, a certain flexibility in terms of frames utilized to depict what the problem actually is and the existence of a lead agency, a policy entrepreneur, or other political leadership (Peters 2013). As a matter of fact there is no single best solution for coordination problems and the w*ays in which successful coordination may take place is very much* sensitive to the environmental conditions under which it takes place (Laegreid et al. 2015).

Existing literature on governmental coordination is primarily dealing with case studies of such efforts – and most often how this went awry (e.g., Mayntz 1980; Edler and Kuhlmann 2008; Koch 2008). Other strands of literature describe general mechanisms of coordination and their relevance and appropriateness (Huxham 2010; Peters 2013; for an overview, see Hustedt and Veit 2014).

Need of Future-Oriented Policy Learning

Grand challenges draw attention to long-term trends and risks thus pointing out that today's decision-making is not allowed to only focus on current questions but also has to cope with upcoming opportunities and threats.

Grand challenge oriented foresight processes offer a future-oriented framework to assist policy makers in managing the uncertainty of future developments by providing spaces for policy, business, and societal actors to come together to better appreciate their mutual positions vis-á-vis various solutions. Oriented on grand challenges new knowledge as well as a new types of learning in the sense of so-called mode 2 knowledge production (Nowotny et al. 2003) is needed by political systems allowing not only experienced based individual but also learning on the level of political systems.

Need of Successful Coordination Approaches

There is however only scarce literature on successful coordination efforts and even less on such cases in which external experts were utilized within reflexive learning process in politics aiming at achieving appreciable outcomes under adverse conditions.

In the following we want to show that the future-oriented approach of participatory foresight is a new instrument of governmental coordination aiming at enabling collective, reflexive policy learning and hereby changing both, the way of policy and societal learning.

In this chapter we will (1) firstly explain the complementary foresight approach as an innovative, multi-method framework for governmental coordination, (2) secondly define human and structural preconditions for successful transformation, and (3) thirdly sum up critical success factors for successful policy coordination towards transforming society. Last but not least we (4) fourthly will draw conclusions on future challenges and directions.

Foresight as an Instrument of Governmental Coordination

What Is Foresight?

Foresight is a conceptual framework as well as a process of prospective analysis and informed decision-making that includes long- to mid-term considerations of likely, possible, or even just thinkable futures (Miles 2003). It joins experts, stakeholder groups, and decision-makers to create channels for communication and to develop a sufficient basis for shaping a desired or avoiding an undesirable future. To this end,

participants arrive at a deeper and shared understanding of impact factors, drivers, their interdependencies, and resultant dynamics influencing the future (Holste et al. 2010).

Foresight is about anticipating transformation and change in different fields (e.g., technological, social, socioeconomical, ecological, or political). Aiming at context governance backwards from future perspective foresight outcomes is expected to deserve the label of innovative quality. Such complex processes of transformation make it essential to combine foresight methodology with principles and techniques stemming from organizational development (Wilhelmer and Erler 2010) (Fig. 1).

In a way, foresight is one answer to a worldwide lack of soft governance strategies dealing with complex and unpredictable transformation patterns in an adequate and sustainable way. The focus is on the increasing need of both economy and policy for generating scenarios and anticipatory strategies (Fig. 1) for improving the basis of today's decision-making.

Earlier phases of foresight (see, e.g., Popper et al. 2007; Eriksson and Weber 2008; Miles 2003) quite commonly focused on the identification of technological opportunities for improving the competitiveness of industries (national champions for comparative advantages). Additional research priorities for national or regional research programs (priority setting), innovation potentials based on frontier research and emerging technologies (horizon scanning), or assessing impacts of technological developments (technology assessment) were mostly elaborated during earlier foresight phases.

Nowadays foresight copes with a variety of societal challenges such as climate change, aging, poverty, environmental hazards, security, or ecologic sustainability. It is expected to provide transformative impulses to discourses held by the public and/or private sectors as well as to condense facts, to synthesize knowledge, and to make insight and recommendations for action regarding the above challenges.

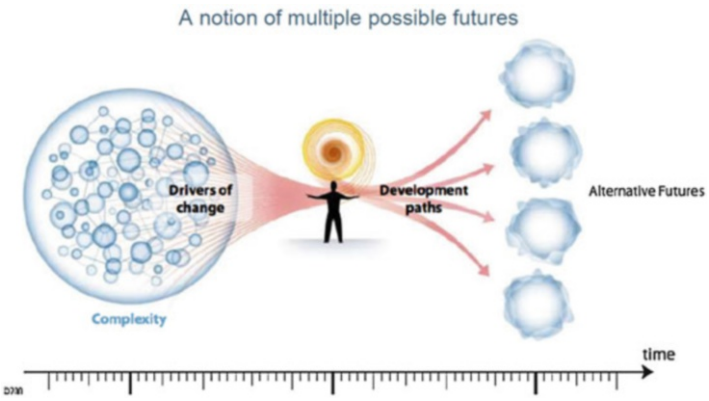


Fig. 1 What foresight activities are for (Source: S. Giesecke; Project ERAlearn; Foresight Training slide 2016)

Participatory Foresight: Future Emerges in Co-creation

Due to the demand to answer upcoming grand challenges we can detect an increasing need for forward looking strategic approaches in policy making and economy.

Foresight allows the

1. Acceleration of change in science and society offering foresight expertise beyond short term horizons
2. Increase of interdependencies and interlinked networks by widening classic planning limits
3. Limitation of room of maneuver of individual key actors by carrying out coordinated action in the meaning of process and result
4. Answer to the demand for concerted orientation and visions by integrating diverse perspectives, disciplines as well as realization and implementation of results while mobilizing stakeholders trough participation

Usually top-down instructive attempts to accelerate change mostly activate resistance of people concerned thus slowing down instead of speeding up. Classic planning strategies start from the presumption that the expertise of a set of people can identify and give orientation for urgent changes to be executed.

In the 1950s and 1960s due to expertise driven technology forecasts foresight followed a top-down technology driven approach. Scientific discourses offered an accepted framework for dealing with future issues. Interdependencies and interlinked networks of diverse stakeholders were not emphasized but neglected as too emotional driven subjective discourses.

Today struggles between disciplines claiming to hold the universal truth of life come to an end as well as the distinction between educated and ill-bred people. The term ill-bred only points to the fact that people marked in that way are members of distinct communication communities or disciplines. Single nations, regions, or organizations cannot create answers to grand challenges and future risks. Decision makers of diverse policy silos and industrial sectors face novel and complex problems deriving, e.g., from global climate and societal changes. This demands for a participatory approach of foresight.

The art of shaping attractive images of future is based on a transdisciplinary combination of knowledge deriving from technological, economic, social, and human sciences and experiences of people and decision makers concerned. The participatory foresight is a silver bullet for intelligent and sustainable decision-making based on the insight that policy advisors never can take a neutral, objective, and external role: whatever decision will be made policy advisors and decision makers will be affected by this comparable to all other people concerned.

Social systems depend on the capability of collective sense making processes. Organizations, projects, and networks are obstructed in elaborating good results if their members start to struggle against each other. If there is no appreciation or comprehension for perspectives and rationales of managers, they immediately lose their capability of guidance and management. Reality becomes what gains an impact

and that is why the intense communication within foresight processes can influence transformation of social systems.

Especially telling success stories gives a baseline for discourses focusing on desirable futures, thereby opening options for exploiting given collective knowledge repertoires of experts and civil society as well as decision makers concerned. This process of communication sparks enthusiasm and intentness to realize challenging actions based on the knowledge that future changes only can be based on past successes. Nobody can drop out from his or her experiences, roles, and contexts: Dialogue-based participatory foresight processes pick up and combine all these corpuses of knowledge and diverse perspectives based on reliance, curiosity, and appreciation for reliable and jointly assessable, future-oriented solutions.

The pioneer of European peace movement Robert Jungk is said to be the inventor of participatory foresight processes in the 1980s inviting ordinary people to discuss with experts of economy, science, and policy within future workshops. Thereby he aimed at strengthening communities and networks of society in order to enable them to take the role of a counterweight to civil servants and politics after the Second World War.

Future is nescience. Although we cannot know what will happen in future, we shape with today's actions our future and create pictures and prospects of our world of tomorrow. The option to look back from a desirable future to the present of society and life allows building backwards scenarios as a frame for future-oriented roadmaps and action plans. If all stakeholders keep their eyes on the horizon of an attractive and desirable future, the pathways for essential actions unfold and keeping their heart open, the feet will follow as if bundles of measures were guided from an invisible hand. Thus foresight processes are able to mobilize huge energy for implementing roadmaps and actions by the means of motivated key players in different sectors of social life.

Surely participation is in need of more extended resources of time and money compared to expert driven approaches. This disadvantage is accompanied by specific benefits: On the one hand, results gain much more acceptance, and on the other hand cross-sectoral, cross-discipline, and cross-silos networks emerge enhancing sustainability in all realms affected. Thereby committed images of future lead to coordinated actions of different organizations in the present.

One of the main benefits of participatory foresight processes is that with only little efforts radical changes of mental models and patterns of behavior of organizations and people can come to reality. At the end of a foresight process stakeholders have transformed and the chance that they change their activities referring to their working environment is rather high.

Related to governmental coordination on the one hand, foresight is used as policy information aiming at more rational decision-making over regions and time by highlighting the longer term and extended perspectives. On the other hand, it aims at advocacy coalition building by building a broad commitment to realization of a shared vision by highlighting a given challenge and gathering support around it. Finally yet importantly, it is implemented as an instrument of social context governance by realizing a hybrid set-up for strategic reflection, debates, and action offering new frames and thus changing old debates by means of a wide participation.

Foresight as an Innovative, Multi-method Framework

In order to be able to navigate through uncertainty, decision makers can refer to foresight framework as a flexible coordination system as well as a box of various future-oriented instruments. Both allow them to gain orientation as well as to start thinking future in a novel mode. Ian Miles defines foresight as a conceptual framework for combining and integrating future-oriented methods in order to support informative decision-making processes (Miles 2003) within a highly complex environment.

In most cases the methodological framework of foresight is tailored to the specific needs of the foresight process as well as to the allocation of resources (e.g., people, expertise, technology, or time). There exists a wide range of such methods and often they are combined in different ways.

Foresight Phases and Method-Mix

Foresight processes on a timeline pass of three phases (Fig. 2):

– *The pre-foresight* can be seen as a scoping state clarifying the goal of what should be achieved. It defines a specific orientation related to economy, society, and

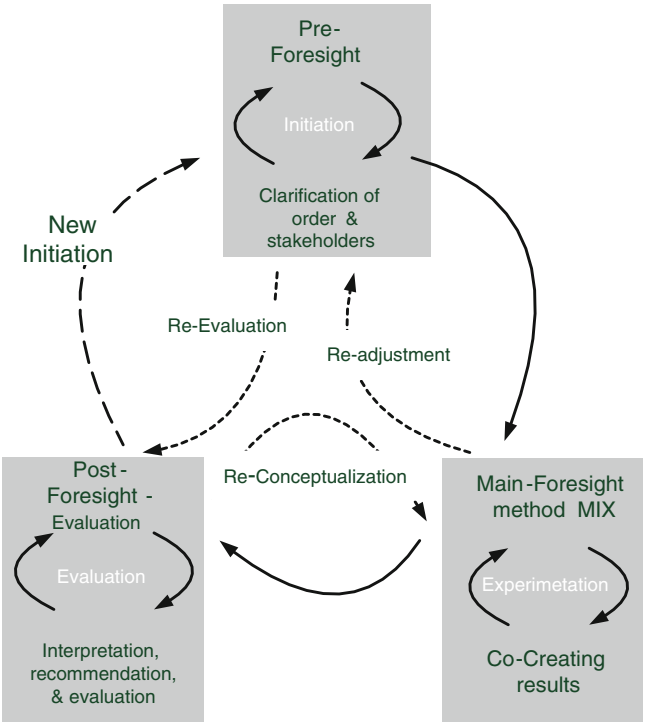


Fig. 2 Circular foresight process (Source: Wilhelmer/Nagel, p. 27)

science and decides a specific scope of time horizon (15–20 years and more) (Mitchell et al. 1997). It sets a specific sectoral problem-oriented focus and identifies stakeholders to be included in the participatory process. Last but not least sponsors like public agencies or private organizations are identified. Related to the recruitment of resources methodologies and methods are identified, a project team with partners and subcontractors is set up and a steering group and advisory group is implemented. Finally a specific mix of methods is fixed and counselors for facilitating the process of learning and experimentation are invited (Fig. 2).

- *Main*-foresight can be seen as a generation state starting with an environmental analysis of drivers and megatrends (STEEPV approach of S-ociety, T-echnology, E-conomy, E-cology, V-alue related) and aims at producing new knowledge by scanning emerging issues, creating scenarios and new visions of the future. Thereby different methods like trend extrapolation, Delphi, story lines, story boards, (forward and backward) scenario building, modeling, visioning, and road mapping are implemented. In order to find context tailored combinations of fitting methodological mixtures, creativity is sought.
- Post-foresight can be seen as an interpretation and action stage elaborating strategies, policy options, and recommendations and building networks for decision and policy making. In addition this phase includes the option for renewal (Miles 2002; Popper 2008) based on evaluation of achieved impacts and identifies aims to be followed up.

In order to support decision makers in setting up foresight processes (Wilhelmer and Nagel 2013) assigned foresight methodologies according to these three phases. Following Popper (2008), one may group all methods into four categories, based on (1) expertise, (2) interaction, (3) evidence, and (4) creativity.

Foresight methods (Fig. 3)

1. Aim at collection and interpretation of experiences and expertise available such as expert panels, interviews, collaborative mapping, scenario building, and road mapping
2. Extrapolate evidence-based knowledge from publications, patents, market- and trend analysis, (agent based) modeling, bibliometric searches, benchmarking, etc.
3. Stimulate dialogues and networking by means of Future Conferences, Open Space, World Café, citizen panels, result galleries, fishbowl conversation, delegation conference, sociometry, etc. (Fig. 3)
4. Unfold co-creation and creativity by means of collecting wild cards, improvization theatre, playback theatre, simulations, role play, science-fictioning, graphic facilitation and painting, etc.

A suitable balance between these categories, as well as the integration into decision-making procedures, is seen as critical not only to reach achieved milestones and deliverables but also to inspire creativity and enhance trust-based co-creation.

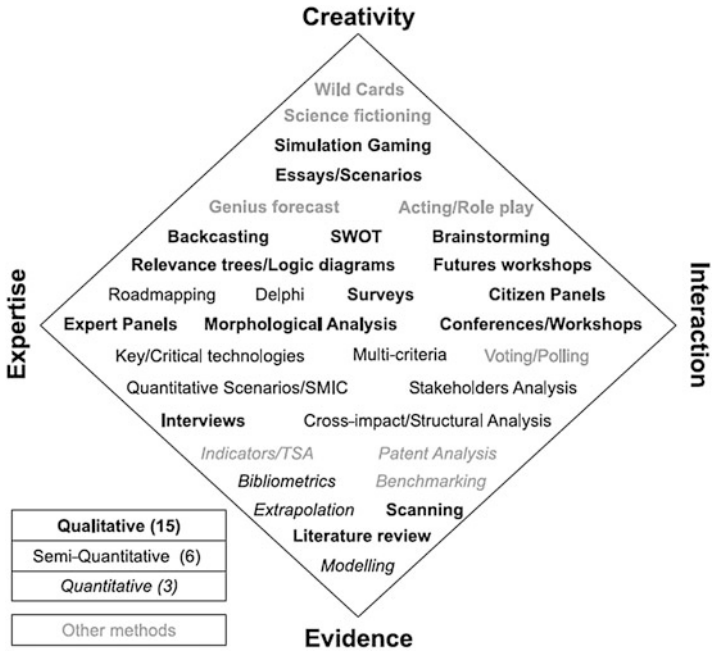


Fig. 3 Popper's diamond (Source: Raffael Popper et al. 2008; Georghiou et al. 2003)

Context Governance via Foresight Architectures

Any attempts to address grand challenges must span a number of long-standing organizational, epistemic, and sectoral boundaries by (1) requiring interdisciplinarity that transcends the boundaries of traditional epistemic communities, (2) cross-departmental coordination and coherence beyond the traditional silos that characterize policy making, (3) multilevel governance approaches that acknowledge the principle of subsidiarity while ensuring coherence between global, regional, national, and local level, (4) cross-sectoral collaboration between various industries, and (5) long-term time horizons to be introduced more explicitly into shorter-term policy agendas and business planning practice (Cagnin et al. 2012).

Social Foresight Architectures

Complementary foresight processes combine both logic and structural elements of common project management as well as structural elements of context-governance deriving from (trans-) organizational development.

Foresight processes are embedded in project frameworks spanning about 12–24 months. Comparable to traditional projects often functions like "client," "project coordinator," "project team," and "advisory board" are applied. From a project perspective, the project coordinator is the person in charge for quality and accuracy of all results to be reached.

As novel structural elements on the one hand a core-team and on the other hand a stakeholder forum including 60–250 people concerned are implemented. The core team is coordinated by the so-called foresight process owner who is the person in charge for conceptualizing and facilitating the overall foresight process. From a process perspective, the process owner as well as the core team can be seen as the heart and engine for conducting an inspiring and effective co-creation process. Therefore, this core team consists of the project coordinator as well as the process coordinator and a person in charge for event management and dissemination. At least one expert, having a good overview on the Foresight goal and its related expertise, should join the core team on a voluntary basis.

In addition a Strategic Steering Board is implemented as a third new structural element: It flanks the overall process, thereby involving clients to an unusual high extent. This allows controversy discussions and mutual learning processes of clients as well as foresight core teams. Furthermore, these steering boards permit the assessment of intermediate results as well as continuous definition and adaption of overall goals. The advisory group offers another set-up for reflexive policy learning including civil servants in the evaluation meetings of researchers stemming from universities and applied research organizations.

The Strategic Steering Board flanks the overall process: A workshop with steering board members taking place before the Visioning forum allows a joint definition of overall goals and the concepts for specific realm like, e.g., "quality of life," "mobility," and "demographic change." Due to the intensive and controversial discussions, impulses for developing analytical models can emerge within this first collaboration. The steering board also evaluates the overall outcomes of the process in a closing Strategic Steering Board workshop, in which identified measures are discussed and last refinements are addressed to the project team.

These structural elements of context-governance (Fig. 4) aim at offering a suitable communication framework for enhancing the unfolding of trust, reliability, and self-responsibility as well as the emergence of novel knowledge. Therefore three different communication set-ups of context-governance are implemented addressing (a) process governance, (b) searches for new information, and (c) transformation of mental landscapes and patterns of the stakeholder forum as a whole system as well as of individuals deriving from diverse home organizations:

(a) *A governance*-set-up consisting of the project coordinator and the core team. This set-up is in charge for conceptualizing the overall process design as well as for conducting and adapting the foresight process.
(b) *A transformation-set*-up composed by project members representing a high range of diverse expertise. Members of this set-up are responsible for generating available information by, e.g., (desk, bibliometric, etc.) searches, patent analysis, and modeling.
(c) A *transformation-set-up* offering a communication framework for all stakeholders involved while also including all functions of the steering as well as development-set-up.

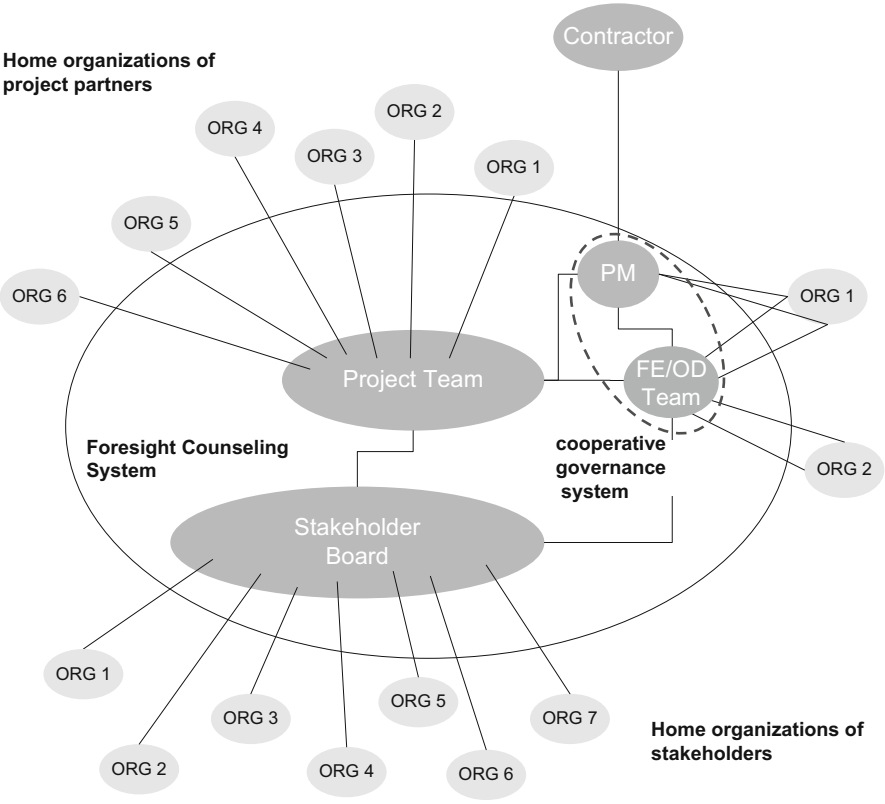


Fig. 4 Social foresight architecture (Source: Wilhelmer and Nagel 2013)

Members of this Stakeholder Forum assume responsibility for moderating and shape process and results by contributing personal experiences and expertise. Besides that a key mission of stakeholders is to reflect intermediate results with colleagues of their "home-organizations" thus spreading and adapting foresight results to local and organizational requirements (Fig. 4).

We use the term of context-governance in the sense of Helmut Willke (2004). Willke points out that social systems are able to learn faster and more efficient than their competitors are, if they learn how to learn and if they decide on a strategic level, what should be learned preferentially. Co-creating novel solutions on eye level with about 60–150 stakeholders presumes a context sensitive step-by-step selection and combination of single foresight methods as well as periodical meta-reflections and adaption of strategic goals and intermediate results.

Thereby the instrument of large group processes and the collective wisdom of all stakeholders engaged show up to be critical for engaging different voices, protecting spaces, balancing interests, and for making connections and coordinating experiments of novel thinking and acting (Cagnin et al. 2008). Especially multiple

feedback loops between all foresight members involved allow mutual learning processes which often result in scanning and identification of solutions as well as in adaption of already existing sectoral, regional, and organizational strategies or institutional, regulatory frameworks long before official outcomes are committed and documented for the official client.

Here this context-governance approach allows policies related to networks and community building as well as to visions, experiments, and learning highlighting coevolution as well as multidimensionality and complexity of multi-actor processes. This form of accountable governance is better able to jointly anticipate and adapt to future, addressing common challenges as well as to spread democracy at a global level (Boden et al. 2010). Last but not least this approach allows transcending boundaries to better address grand challenges and utilize multiple levers for shaping policy learning and societal change. Context-governance as a coordination effort thereby enhances communication and understanding between policy silos thus supporting the emergence of an effective policy mix for innovation and change (Cagnin et al. 2012).

Content and Timeline Driven Foresight Architecture

Every foresight process is tailored with respect to its realm and appropriate goals. Regarding the co-creation process, foresight processes consist of offstage elements (preparatory steps such as desk research, surveys, modeling) and on stage elements encompassing several Stakeholder Forum workshops. These forums see the meta-reflection of goals and methods, the elaboration of analysis and co-creation of diverse images of possible futures, and the assessment of intermediate results and estimated impacts.

Usually foresight processes are structured around four to six "on stage" stakeholder forums bringing together stakeholders from industry, research, civil servants, nongovernmental organizations, etc. Stakeholders are participating during the overall process, serving as hosts within dialogue rounds, discussing with strategic targets and optional measures on eye level and co-creating a creative visioning and scenario building process.

In order to allow a glimpse of how a viable foresight process could look like, an optional "on stage foresight process" is outlined in the draft concept see below:

(a) *Kick-Off of Stakeholder Forum: "What for Foresight? – A joint departure"*
Tasks: framing the scope, clarifying roles, discussing and agreeing objectives and steps, providing basic information about both participatory foresight approach and foresight concept, outlook to dates and venues.

(b) *Scenario 2050 Forum: "Thinking alternative futures"*
Tasks: Identification of main societal, technological, economic, environmental, and political drivers in specific life contexts (trend-analysis, environmental-analysis). Mental future journey by a guided imagination enabling stakeholders to change their view from present time to a future perspective of 2050. Building future trajectories and story lines providing a paradigmatic base for developing guiding

scenario-frameworks for storyboards. Embedding "personas" in concrete scenes of (un-)desirable life scenarios of 2050.

(c) *Vision Forum 2050: "Dreaming a desirable future and breaking down future orientation."*
Tasks: Performance (improvization theatre) and assessment of approximately five life scenario sketches addressing key messages of about four best case and one dystopia scenario to the stakeholders, allowing both, a humorous working atmosphere in the large group as well as the deduction of qualitative objectives. Visioning process of a desirable (normative) future and deduction of qualitative and quantitative objectives 2050 as well as guiding long-term issues for subsequent road mapping process.

(d) *Roadmap Forum 2050: "Paradox planning of uncertain and unforeseeable futures"*
Tasks: jointly identification of transformation goals and drivers as well as change agents in the field; road mapping of bundles of measures (functional perspectives, information types) and strategic planning. Robustness check of bundles of measures.

(e) *Action Plan Forum 2020: "The end of conceptualization as starting point for action!"*
This forum aims at achieving overall foresight objective by putting in place measures from various policy fields. Existing policy measures are analyzed and gaps in the policy landscape are classified and identified. Afterwards demand stemming from policy analysis carried out before "on stage stakeholder forums" is defined, and policy recommendations and implementation plans are defined.

Societal Changes Deriving from Co-creation

Paradox of How to Decide Under Uncertain Circumstances

Modern systems are characterized by a complexity, overburdening actors from policy, economy, and science. Especially decisions dealing with long-term challenges are affected by this phenomenon. Today's decision makers face the challenge to, on the one hand, have to align their organizations to a future and on the other hand have to accept that future development as a principle is neither foreseeable nor projectable. This contradiction cannot be solved at all. Accepting that solutions can only offer temporary optima for specific contexts, this paradox provides continuous energy to revisit decision-making for complex, grand challenges. The task of decision makers is to continuously deal with this constitutive paradox of future in a smart and constructive way.

Starting from the presumption that future cannot be forecasted but only shaped in co-creation opens a space for maneuver to consciously navigate through nescience and uncertainty. Dealing with uncertainty is in need of clear cornerstones to allow navigation full of relish. Additionally open and flexible coordination systems (clear scopes of foresight) and governance set-ups (foresight architectures) are needed for

guiding strategic discourses in organizations and policy as well as a toolbox including a high variety of instruments (foresight methods). This allows to experience ourselves as deep-rooted in unboundedness as a principle.

Based on constructivism we understand foresight as a communication process allowing future-oriented decisions in the present for the present. Methodologically approaches such as scenario-development, robustness checks, and wild cards allow balancing necessity and impossibility of planning future. Results not aiming at integrating both quickly are passed by just by this reality, which should have been caught through decision-making.

A specific selection of a foresight method-mix aims at offering all stakeholders involved the option to better understand estimated, not intended and unexpected future developments. Thus foresight framework allows simulating possible futures and their impact on society, market, investments, etc. by means of intellectual gaming. Thus co-creating futures offers a collective rehearsal for viable transition in the present. Thereby created robust scenarios allow identification of interdependencies between drivers as well as unwanted impact of evolutionary patterns in the upcoming future. Future remains uncertain but on a higher level of information (Wilhelmer 2012, page 8).

Tomorrow Today

For shaping future-oriented, reflexive processes of policy learning one should take into account how humans can deal with past, present, and future.

Past and future are no realities but grammatical principles of languages. Human beings only can live in the present. Only story telling in an oral or written form makes glimpses of yesteryears and possible futures accessible. Thus past and future can be seen as construct of our communication. Humans only can live in present as a principle (Schmidt 2004). Stories and illustrations of past and futures are always constructed by special observers in a specific context based on a unique motivation. Mutualizing these stories allows also mutualizing appropriate rationales and assessments affecting our actions in daily life. Modern brain research points out that our biographical memory derives from combinations of faultily mementos (Markowitsch 2013). Thereby we are never allowed to forget that humans experience the mode of stories as if they are experienced on a physical level. This leads to storytelling immediately having positive or negative impact on our nerve system thus influencing the mental state of all people affected by these stories. The body as real happened injury (Schmidt 2004) experiences a verbal threat of violence. This makes story telling regarding present, past, and future times such a powerful instrument for exercises of influence and interventions aiming at transformation.

Milton Erickson (1954) calls this human's capability to go for journeys through time "pseudo-orientation in time" or "time-progression." This hypnotherapeutic procedure allows the experience of anticipated desirable future incidences as present on an emotional and physical level. This empowers people to orient themselves towards a new and desirable goal. The flow and power inherent to the anticipated

solution delivers energy to change even favored dysfunctional patterns of thinking and acting. In this procedure, the desirable future not only is critically questioned within Foresight Scenario Workshops but also lively experienced and anchored in reality while co-creating attractive future visions in large stakeholder-group workshops.

New knowledge and technologies sooner or later do not fit to traditional, old views of the world and orientations deriving from them. Old ideas of man and concepts of enemies embedded in the collective memories of families, clans, tribes, and ethnic groups have to be revised and adapted to new circumstances. New goals have to be elaborated.

Humans, organizations, and societies organize themselves by means of mental images and storytelling like myths, legends, religions, etc. These stories enhance the cohesion of social systems by indicating desirable internal arrangements and regimes. Long-term oriented images are not precondition for survival. Following Gerald Hüther (2010), they are the most worthwhile elements of our life especially in turbulent times when social structures threaten to burst. Brain research tells that collective positive images can give urgent orientation in times of disruptive cracks and the necessity of reshaping our living environments. Confidence and reliance is not only an essential source for life but also source and driver for social transformation processes.

Turbulent situations of radical change highly challenge these demands for self-organization and are in need of powerful internal images encouraging and empowering humans such as employees and decision makers of all societal sectors. Following Helmut Willke (1998) developing a joint desirable vision doesn't aim at obedience or behavioral change by dint of group dynamics and group pressure. Contrariwise, the insight those humans unfold surprising potentials when focusing on true visions works as a guiding principle of foresight processes: people learn on their own motivation beyond pressure and instructions.

Embedding concrete elements of current contexts into vision building processes allows experience and experimentation of future in the present. Learning processes referring to specific life contexts are immediately interwoven with daily routines and thus cannot be neutralized and dissociated from one's course of actions. This mode of context-related solution orientation quickly can lead to changed patterns of thinking and acting and thus visioning processes can be seen as instruments of soft governance for all social systems.

Following this logic, vision building cannot be conducted top-down but only can be co-created in a joint bottom-up process. Vision building therefore is in need of new participatory varieties of experience-based mutual learning and coordination processes (Wilhelmer 2013).

Change Is What Happens Before Decision-Making Took Place

Long before selected formal results of traditional foresight processes are implemented in transformation processes, research agendas, strategies, white papers

or regulations, transformation of thinking, and acting of stakeholders involved have already happened. In short, change is what happened before one's decision that it should happen.

Participatory foresight-processes initiate mutual learning processes and the emergence of informal "cultural islands" (Schein 2010). These cultural islands operate as transformative spaces marking rooms for incubation of new patterns of thinking and acting, based on novel roles and rules of the game. Thus, "cultural islands" operate as "niches" marking the beginning of transition processes. Within 1 or 2 year lasting foresight processes' actors oscillating between the two worlds of daily routines and "cultural islands" have the option to critically question and deepen insights and learning in practice. Thus, participatory foresight allows rehearsal for transition within protected transformation spaces as well as continuous assessments of appropriate findings and insights thus driving transformation processes inside out and changing cultures and values of decision makers in a sustainable way.

Similar to other social processes of transformation participatory foresight works only by combining top-down and bottom up approaches: Without a client, giving money there is no foresight process happening. On the other hand, the precondition for a high quality of foresight results is the inclusion and co-creation of a high variety and diversity of stakeholders concerned. Only this combination allows high quality and impact of foresight processes for policy learning and societal change.

Relevant societal renewals are in need not only of powerful future images and confidence but also of legitimacy and implementation power. Policy and industry, aiming at sustaining their power and market success, necessarily focus on their voters respectively customers in order to increase the positiv impact on their election/sales forecasts. And these customers and voters are per definition the key stakeholders of social systems and also of foresight processes. The focus to long-term changes has never supported political parties to win an election.

Foresight processes mark a social and political antithesis to short-term thinking and the habit to stick to one's own, singular interests. They allow transparent, opposing models of coordinating democratic processes contrary to autocracy, concentrating power only in the hands of one person beyond external legal restraints or regularized mechanisms (absolute monarchy, dictatorship). Outsiders stemming from lower class tend to call for dictatorship in contrast to well-educated people of the middle class. The latter try to live and work in periphery to autocratic structures and centers of power (Senge et al. 2011). Neglecting centralized political structures thereby is not seen as a weakness but as a chance and room of maneuver for transformation. From a democracy policy perspective, aiming at well fare policy and societal change there is a need of inclusion of a wide range of people concerned. Thus, transformation and change is not claimed but jointly shaped.

Changing between perspectives and diverse realities fosters willingness to critically question one's own perspective and knowledge thus widening the view towards complex interdependencies. Especially it sharpens the perception of today's needs often representing tomorrow's critical success factors up till now not served by policy or economy. There is a need to lift and utilize existing tacit knowledge and innovative ideas for society referring to social innovation "by its ends and needs".

We Are the Change

Stakeholders are central for this approach. The English language defines stakeholders as partners and/or owners of a stake referring to a specific "yes or no" question. In its essential meaning the word "stakeholder" addresses the practice of participation in the sense that stakeholders perceive themselves as having a legitimate claim of partaking referring a specific decision-making process.

Following Robert Jungk, stakeholders were essential after the Second World War to take responsibility for shaping the after war society beyond waiting for actions deriving from policy. In this perspective, shaping society is a central, original task of every citizen of civil society.

Nowadays stakeholders have a very important role in view of finding adequate answers to grand challenges in democratic manner. The entrepreneur and pioneer Paul Hawken points out an increasing role of nonprofit organizations since the 1990s: Counting international nonprofit organizations Hawken indicates an increase from 40 organizations in 1948 to 700 organizations in 1992 without counting nonprofit organizations on national level. This development is seen as one of the greatest social movement in the history of humankind. His hypothesis is that this movement reacts to the increasing awareness of urgent threats deriving from climate change and limited natural resources of our planet.

Besides economy and policy, nonprofit organizations have developed to an influential and effective power referring to issues of society, research, R&D policy, and economy. For example, Shell had to stop its decision to sink its old oil platforms after protests and actions of Greenpeace, and Nestle had to reduce its sale of milk powder when NPO highlighted an increase of childhood mortality in developing countries because of decreasing breastfeeding. For instance, in Austria a ministry was forced to change its vote for allowing pesticides on European level after a lot of media and people protested against permitting this chemical substance claimed to be responsible for mass mortality of bees.

In lieu of top-down government and control nowadays, policy is confronted with an increasing demand for novel governance procedures allowing coordination of widespread negotiation processes with and between stakeholders (Wilhelmer 2012, page 7).

Governing Social System from a Future Perspective

The development of explorative and normative visions is an essential focus of participatory foresight. This exercise aims at supporting decision makers in shaping preconditions for a desirable future in our present. Especially the long-term orientation of participatory foresight processes unfold novel spaces for maneuver: In a knee-jerk reaction, many people refuse questions addressing circumstances of 2060 in 2016. Most of the people suppose that future for their lives can only be predicted in a span of three to maximum 10 years. Beyond that is said to be unthinkable and therefore not relevant.

Nevertheless, just this question addressing the next 50 years unfolds radical novel spaces for creativity. Many stakeholders imagine themselves to be beyond 80 years of age, thereby facing radically changed environments and physical as well as mental conditions. Others expect not to live any more in a time 50 years ahead. And especially this view beyond one's individual death opens new perspectives regarding the evolution of generations, societies as well as our planet as a whole. A new space for experiences unfolds far beyond current roles and contexts offering new options of freedom. We assume this to be one of the reasons why people with diverse social and ethnic background and gender, belonging to different generations engage joyful within such vision building processes. Actually happiness occurs mainly when our view – limited by the pressure of problems to be solved on a daily basis – widens again and our heart opens generating a lot of ideas just like bubbling from a deep well. In magic moments like these, reality can be perceived again in an unbiased and unprejudiced way as if it would be created in a completely new way – as if a curtain would be drawn aside. The mind becomes free and on the mental stage fantasy and engagement emerge.

Within plenary sessions magic moments like that sometimes are described as "refreshing similar to having a sauna" or as a touching experience of membership to a group dealing with central questions of human life. The feeling is that what happens really matters to all of us and that it essentially depends on every single person.

Explorative future visions focusing not on the dystopia of apocalypse but on visualizing existing potentials and knowledge open a creativity space for visions, which at the very beginning seem to be unlikely. To this effect the project team of the foresight process "Freight vision Europe" was surprised by this phenomenon when about 120 stakeholders deriving from different technology platforms, oil and automotive industries, infrastructure providers, policy, and science, decided quantitative objectives which at the beginning were rejected as being illusory. Eighty percent decrease of greenhouse emissions, 80% decrease of congestions, and 50% decrease of fossil fuels usage: This courageous self-commitment allowed the project consortium to look for novel solutions in the subsequent development of backwards scenarios.

Coordination of decision as well as implementation processes backwards from future perspective assumes confidence of all stakeholders concerned. This confidence can only emerge based on images of society supporting and encouraging a continuous evolution of resilient and adaptive societies among unforeseeable dynamics of a complex world.

Forward-looking foresight processes allow making up future journeys and stories in a way that activate meta-reflexion of interests and solution potentials of stakeholders aiming at preparing pathways for desirable futures. Governing from a future perspective looks for leverages to activate transformation. This demands co-creatively developed paths towards attractive futures where no way is allowed to claim to be the only silver bullet. Sustainable capabilities of dealing with confidence, curiosity, and uncertainty are thereby essential, putting formal results such as roadmaps and action plans into perspective of rather short-term validity (Wilhelmer 2013).

No Time Left for Serving Particular Interest

Lobbyists earn money for fighting for particular interests. If they can't drive policy by economic power they try to pay off civil servants well known from European as well as national level. Foresight processes have the power to stand up against, e.g., by means of transparent co-creation of future images. Precondition is a transparent, co-creative process of lion-hearted actors that observe attempts at intimidation as confirmation of their work.

A Scottish officer standing up to attacks of a European railway organization highly impressed me: At the end of an almost 2 years lasting European foresight process, a paradox situation occurred in the fourth Stakeholder Forum consisting of 110 people. Although it turned out clearly that CO_2 emissions were primarily caused by the "street" (individual and freight transport), this result was not fought against by representatives of infrastructure providers as well as automotive and freight industry. Contrariwise, this railway organization stood up against the results based on the rationale that money would flow where the hugest problems were identified. Following this rationale the "rail" would have had a drawback regarding to public investments in the upcoming years.

In consequence, rail organizations across Europe lobbied against the EC officer in charge for this foresight process. This led to replacement of the EC officer who was moved to a department taking responsibility for similar issues and projects thus continuing his work as before.

Furthermore, the rail association threatened to leave the final conference in case the officer would attend the final conference. When at the end of the project the Scottish officer attended the final conference, the railway association didn't leave but were faced by lessons learned: not the project consortium (about 30 people) but 90 stakeholders put the lobbying association into perspective arguing that so tight to an overall climate catastrophe there would be no more space of maneuver for fighting particular interests. Contrariwise, only coordinated actions could preserve Europe and the other continents for irreversible damages.

Unintended this lobbyist action helped to spread the results widely: the report was read by an unusual huge amount of EC representatives referring to different hierarchical levels thereby widening publicity for all foresight results. In consequence, many parts of the result were included in the famous European white paper supporting official consultations with national governments.

During the closing party of the project consortium, the Scottish officer told the story of his family: His grandfather served in the British Mint thereby uncovering a case of corruption. Subsequently he had hard times during work life as he was outlawed and avoided by all of his colleagues. Finally, in the end of his work life he experienced an extraordinary compensation: He received a knighthood from the queen as tribute for his engagement for the kingdom. Due to his familiar tradition of courage to stand up to one's belief, the Scottish officer interlinked the fight against his engagement for limiting climate change with the struggle against his honorable grandfather. Thus, the turbulences did not serve as symbol of weakness but

contrariwise as marker for individual success: Both men shaping the transformation of systems within different times and contexts.

Foresight processes need both collective intellectual challenging analysis as well as emotional touching dialogues and, of course, brave entrepreneurs perceiving turbulences not from the role of victim but from the role of a shaper of change.

Powerful collective images and success stories support and enable societal transformation more effective and sustainable than assumed in political science discourses: This is good news of participatory foresight processes (Wilhelmer 2013).

Conclusions

Summary

The term "grand challenges" can be seen as a symbol for the complexity of our world. This symbol stands for the unmanageable interdependencies and unforeseeable dynamics in globalized social systems. Thus, it marks the necessity of continuous responsible and social transformation and adaption by means of governmental coordination and societal engagement.

On the one hand, coordination efforts of policy and civil society seem to be more promising when stemming from a future perspective back to the present, based on confidence and powerful images of desirable futures. On the other hand, coordination efforts have to enable experience-based, reflexive learning of policy as well as of all stakeholders concerned in the sense of learning how to learn (Willke 2004). Contrariwise to "single loop learning" addressing simple adaption to changed environments (Argyris and Schön 1999), "double loop learning" includes not only the change of action strategies but also a critical assessment of norms and values embedded in organizational set-ups. This assessment starts from an observed impact triggered via modified actions. Similar to Willke, Bateson (1988) addresses meta-reflexion of beneficial and obstructive context conditions as a mode of the so-called Deutro learning or second order-learning.

Second-order learning directly interferes with conditions of learning contexts thus giving hints to how communication set-ups have to be shaped in order to allow mutual learning on how to learn and thereby transform oneself in a desirable manner. Referring to policy coordination these learning contexts are interlinking diverse organizations, institutions thus building so-called hybrid structures for societal, and policy learning. Following this perspective, coordination effort of policy such as foresight processes or the new formats of "Living Lab" or "City Labs" can be seen as hybrids aiming at network governance, community building in the sense of mutual learning, and radical change of actors and actions. Living Labs are increasingly popular strategies to address sustainability challenges by providing a holistic and iterative framework for the coproduction of knowledge (Evans et al. 2015).

Learning contexts are not beneficial by themselves but have to be set up and shaped in an appropriate way to allow changing roles and rules of the game as well as values and mind-sets. Organizations offering participatory foresight as an instrument

for reflexive policy and societal learning have to know and follow six main principles regarding the implementation of its role within a cross-organizational communication. These principles are key for allowing coordination of cross-organizational communication and refer to the question how to implement the role of foresight in a supportive way fostering mutual learning and self-transformation processes of a big range of highly diverse organizations and institutions.

In the following, we want to highlight six success criteria regarding a successful role of foresight teams in the interplay of cross-organizational communication. Thereby we follow the main findings of KoStratAktil case study (interministerial working group being the client of a foresight process regarding "life quality and activity in the context of demographic change in 2035") carried out in Austria 2015.

Case study's Lessons Learned: Critical Success Factors for Policy Coordination

Future-Oriented Approach

Dealing with incommensurable, i.e., insolvable contradictory logics, demands the introduction of a "third party" being attractive for all actors included. Foresight processes invite all stakeholders to take up a future perspective lying in a long distance from now (e.g., 2035). This allows both to jointly define a vision of a desirable future and to free oneself from daily obligations and constraints interlinked with the individual, specific function of the organizational/institutional background.

The benefit of this approach is to open a space for developing a trustful collaboration culture between all stakeholders – even if they come from institutions with antagonistic relationships to each other. Future approaches replace competition between organizations with cooperation aiming at partial realization of desirable futures.

Regarding the KoStratAktil case study this approach worked well:

Representatives of ministries as well as of NGOs and industry jointly developed story lines and storyboards before playing sketches addressing key messages of the joint desirable future. Regarding the visioning process, we became aware of the so-called lock-in phenomenon of social communication. This phenomenon indicates the principle condition of humans that they cannot see what they cannot see: Visions include wishes and demands deriving from people's experiences in the past. The decontextualization of these wishes can positively be seen as the extrapolation of principal human needs providing both sense and motivation of human lives. On the other hand, visions also reflect images of possible futures stemming, e.g., from diverse public and private media or neighborhood communication, thus reflecting the common mind-set as well as blind spots of the people included.

Reacting to this phenomenon the foresight team added complementary perspectives from future search to the jointly elaborated visions resulting in narrative stories of future scenarios. In doing so foresight teams have to take into account that they also underlie the principle not to see what they do not see.

Policy advisors should not underestimate this step, as the challenge here is to transform knowledge and expertise deriving from alternative future studies and research into co-creative story writing, i.e., in the specific creative format of future stories without changing the key messages of the scenarios stemming from the stakeholder process.

Transdisciplinary Approach

A user centered approach in policy design requires resigning from familiar "expert talks" and instead developing a joint language, e.g., regarding the definition of key terms, key objectives, and cross-cutting issues.

This requires getting beyond expert driven competition among disciplines and between advisors and experts from other domains with respect to "truth" and "relevance" allowing a focus on multiple dimensions of the social system. Researchers as well as experts from public authorities, NGOs, and industries have to change their communication mode from "telling" to "asking" and from "claiming" to "mutual learning," which often turns out to be a challenging exercise.

Policy advisors should recognize the importance of including diverse perspectives of the interministerial as well as stakeholder groups inside their team, thus mirroring diversity and complexity of their environment (Biegelbauer 2015).

This demands an investment of more time than usual in clarification processes within the project team itself. Project teams often are challenged since expert organizations frequently are not really used to intensive teamwork and it is difficult to invest more time because of organizational circumstances. Risk-management in this case has to focus on a forward-looking project plan in order to avoid misunderstandings and conflicts deriving from shortcuts in communication processes.

Participatory Approach

Foresight projects are not per se participatory. Aiming at policy coordination however, a participatory approach allows the inclusion of multiple stakeholders' perspectives and contributes to broaden the impact of RTI policy outcomes.

The main asset of a participatory approach is to experience inspiring mutual learning processes thus allowing the transformation of mental models and mindsets resulting in the change of daily practices. Ideally by doing so, a system transition on a social level has already taken place before results of foresight study are fed in policy design and implementation processes. This fosters the quality and sustainability of subsequent implementation efforts as multipliers have already changed their view from critical questioning to active support of new programs and policy actions. Finally yet importantly, this approach increases the legitimation of policy design outcomes generated within the framework of a representative democracy.

A disadvantage of participatory processes is that they require more time compared to traditional top-down policy design processes, often going by enlarged costs (venues, catering, etc.). Besides, these processes need open-minded, engaged policy makers not being afraid to get in touch with, e.g., citizens, NGOs, and industry. This

serves as both requirement for and enabler of the change of traditional mind-sets of policy makers and stakeholders.

(Trans-)Organizational Development Approach

The OD approach allows to build an appreciative cooperation culture as well as to tailor the concrete, context-sensitive multi-method approach by answering the needs of the specific framework of a foresight process (e.g., objectives, target groups, previous knowledge basis, available research results). This allows implementation of both creative and interactive methods for engaging and empowering people concerned as well as the implementation of analytical methods deriving from research and policy design/evaluation processes.

Thus, the organizational development process initiates meta-reflection and self-organization of the project team by navigating through contradictory logics and power struggles. This allows both expertise and analytical methods as well as social mediation and negotiation to be utilized as equal by valued parts within participatory policy design.

Applied research organizations or universities serving as political advisors support policy design processes often. The primary aim of these expert organizations is to generate new knowledge on content side. This is why they often are not used to implement participatory stakeholder processes or miss skills required for conducting (trans-)organizational processes. Expert organizations often underestimate organizational development being a social research discipline by itself. Advisors then try to utilize its methods by means of manipulation: in the sense that OD methods should help to increase acceptance of their expertise by policy makers and end-users without taking into account the necessity of mutual processes allowing innovation deriving from co-creation processes.

Advisors are recommended to integrate a neutral OD expert and mediator in their interdisciplinary team either as a member of the expert organization or as a freelancer supporting the project team by overcoming obstacles such as those mentioned above.

Complementary Approach for a Research Design

Transdisciplinary and multi-method oriented policy coordination and policy design processes require a context tailored complementary combination of both content point of view and mediation/social process (Wilhelmer 2009).

In the KoStratAktil case, the policy analysis laid bare strengths, weaknesses, and opportunities of the Austrian research and innovation system. Through expert interviews, important policy issues not yet targeted by government policies were detected. Without gaining an overview of strengths and weaknesses, no recommendation of enhanced interministerial coordination within cross-cutting research areas could have been suggested.

The expertise of the stakeholders included in the participatory foresight process allowed assessments on plausibility as well as completeness and up-to-dateness checks: after all policies are not carried out by policy makers, but by, e.g., the civil service, experts of companies, NGOs as well as care and research organizations.

Moreover participatory processes are able to use tacit knowledge of stakeholders related to present and future programs, projects, and actions thus serving as an additional information source as well as quality manager for foresight study outcomes on content side. Thus, successful policymaking requires advice including and balancing scientific analysis as well as creation and usage of appreciative and trustful relationships between all actors.

This requirement often challenges expert organizations, which – because of their main objectives and history – primarily focus on the generation of knowledge and content.

Special Framework

Successful policy coordination among other things needs an organizational framework such as RTI strategies on European and national levels, which provide for a reason to engage into coordination activities and a set of norms and rules for the coordination process.

In addition, the awareness of policy makers for the need of early warning systems is demanded in order to detect and identify upcoming threats and chances and to aim at the extension of resilience and robustness of cities, nations, and countries.

Funding for supporting activities such as a foresight process is also very helpful. For the coordination in general, but especially for participatory activities the presence of the ministerial decision makers is of utmost importance. In the case of the KoStratAktil project, the willingness of decision makers from the ministries to engage into this process was a sine qua non condition for fostering policy coordination between the ministries.

Future Directions for Governmental Coordination and Policy Learning

Our overall conclusion is that coordination of diverse organizations as part of governance needs all (a) reflexive policy learning and transformation of policy makers and political institutions, (b) learning and transformation of advisors and university/research organizations in the field of policy advice, and (c) learning and transformation of stakeholders from industry and civil society.

Especially the mental models of policy makers, i.e., the way they see their social and institutional environment, partaking in coordination activities, have to change in order to overcome well-established practices embedded in institutional rules, norms, and values.

Yet coordination can only be enhanced if all included partners are willing to critically question their own mental models and knowledge developed over the years as well as to change their roles in policy advice from top-down and expert approaches to an enhancement of co-creation and mutual learning.

A perception of the necessity of coordination is part of the motivation actors need to engage into coordination efforts, which may question their mental models and long held beliefs as discussed above.

Societal Transformation in Need of Hybrid Co-creation Set-Ups

Due to the circumstance that dealing with complex situations demands comprehensive efforts of a wide span of organizations and institutions concerned, we can claim that new, hybrid formats for interlinking diverse stakeholders in co-creation and coproduction processes are strongly needed.

Thus, participatory experiments with formats like foresight processes, living labs, city-labs, policy labs, etc. are both increasingly needed as well as popular in applied research. For instance, applied research organizations and universities more often use living labs deriving from user-driven innovation nowadays in order to allow co-creative experimentation and implementation of new technology (e.g., ambient-assisted living, smart grid, smart meter, smart mobility) by means of experts and private, public, or industrial users.

We would like to emphasize that applied research in the sense of testing living lab set-ups regarding its usability for cities and national governments is highly demanded. Besides new guiding corner stones and success criteria are needed to allow an important step forward to implementing various innovative formats of governmental coordination in practice. Henceforward city labs in this sense could bring together not only civil servants of various policy silos but also stakeholders concerned by different realms of policymaking.

Nevertheless, coordination efforts do not only need the development, rehearsal, and assessment of novel hybrid formats of governance but also the extension of beneficial framework conditions for their implementation.

Societal Transformation in Need of Environmental Preconditions

In case of coordination failure, it can make sense to revert to hierarchy in order to create framework conditions supportive to coordination (Laegreid et al. 2015; Voets et al. 2015).

In the following, we will try to define several contextual preconditions on the levels of (a) communication and co-creation and (b) structural and institutional preconditions aiming at widening policy and societal coordination in our today's world.

Preconditions Concerning Communication

In order to foster, e.g., interministerial working groups or comparable hybrid coproduction set-ups, new structural elements have to be committed and implemented allowing the share of costs and benefits of the coordination activities. In this perspective, it turns out to be important to create a cooperative game resting on a positive sum strategy (Hargreaves Heap and Varoufakis 2004).

Put differently, to overcome negative coordination, as part of which actors protect their stakes by not crossing the borders to other actors' competence fields, and arrive at positive coordination, in which actors are ready to change their perceptions and engage into cooperation, trust in cooperation and coordination has to be built.

Another important issue is the flexibility to change frames, which are utilized to depict what the policy problem, i.e., the reason for coordination activities, actually is.

The representatives of the different ministries usually offer differing understandings of which elements would be more or less important, with natures and functions of their home institutions playing an important role in their preferred definitions. To create a common ground by meaning-making, i.e., arriving at definitions largely shared by the group, is an important step and not easy for most of the members of the interministerial working groups as it afforded the above flexibility to work on the problem frames of the group.

Institutionally Preconditions

An important factor for achieving governmental coordination is the existence of a lead agency, a policy entrepreneur or other political leadership. If there is no sustainable interest from the side of politicians in innovation and research policy, it means that there is also no political leadership aiming at going beyond short-term issues as well as hierarchical organization set-ups and top-down strategies.

Spreading the practice to more often implement interministerial working groups for realms regarding cross-policy issues can widen the experiences of civil servants that at the end of the day there is no political backing existing of coordination initiatives. This gives a room of maneuver to co-create and implement strategic guiding issues and goals from a future perspective in programs and regulatory of ministries. Entrepreneurial attitude of civil servants serves here as an important precondition for utilizing the new freedom as a chance instead of excessive demands. On the other hand, these interministerial working groups should not stand-alone but be embedded in anti-hierarchical communication architectures interlinking top civil servants with their entrepreneurial group. This should allow both (a) to invest money in participatory new formats and (b) to allow mutual learning of both the entrepreneurial as well as the top civil servants.

Epilogue on Knowledge Democracy and Quality of Democracy

Looking at the policy cycle (see Fig. 5) we can see that governments are in charge of experimentation with and implementation of policy instruments and R&D programs. This requires the coordination of highly distinct organizations from different sectors, i.e., to continuously deal with complex situations. Therefore, coordination of policy needs both, individual and system learning.

However, how can system learning and thus societal transformation be provoked within political systems?

Aiming at transformation we need both: Firstly, transformation demands experience-based individual as well as system learning on eye level by means of co-creating powerful images and sustainable action plans of desirable futures. Secondly, transformation needs learning of the political system as a whole, provoked by feedback to the quality of democracy. As empirical research has to build on indicators deriving from democracy theories, its feedback brings up criteria for quality of democracy to public discussions.

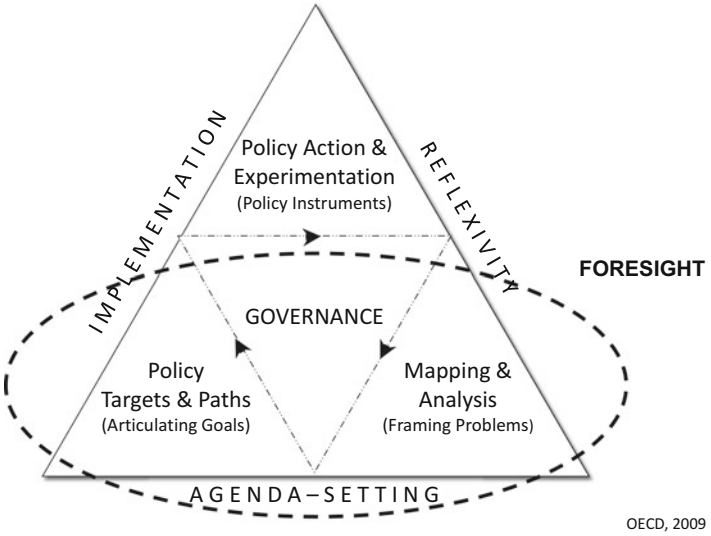


Fig. 5 Integration of foresight in the policy cycle (Source: Adaptive Foresight; AOM presentation Wilhelmer 2012)

Reflexive system learning in both cases does not only address the political system but also its social, economic, and ecologic context. This makes the criterion of sustainable development such an important basic dimension for transformation as well as for Quality of Democracy besides the other dimensions of freedom, equality, and control (see "Quadruple Structure," Campbell et al. 2015).

In order to orient themselves towards learning and transformation, political systems are in need of external impulses. These impulses can derive from both (a) an evaluation (audit) of quality of democracy and (b) informal and formal results of forward looking activities such as participatory foresight processes.

Quality of Democracy Provoking Political System Learning

Within innovation and political systems, incrementalism often leads to lock-in and path-dependency along trajectories that can be difficult to escape, even if a consensus exists that alternative trajectories of paths would be more beneficial to follow (Cagnin et al. 2008).

This is where a meta-theory of democracy – interlinked with democracy measurement and a systematic approach of evaluation – turns out to be a crucial driver for system transition. Aiming at maintaining quality of national democracies by global comparison of empirical quality of democracy, *Democratic Audits* (e.g., by IDEA; Campbell and Carayannis 2014) aim at provoking democracy learning (Campbell et al. 2015) outside in.

Lock-in has to be born in mind when linking evaluation results on lacks of democracy to discussions about quality indicators deriving from the Quadruple Helix Model (see Campbell and Carayannis 2014) in order to allow system learning. Systems never know what they do not know: Accepting this as a condition sine qua non allows both appreciation for the present as well as challenging status quo in order to open future path for sustainable developments. Proactively surveying future alternatives replaces resistance, deriving from not-invented-here syndrome by energy for change.

However, forward-looking activities such as foresight processes allow understanding and mutual learning of external feedbacks from democracy research by offering a communication set-up to overcome resistance in favor of new opportunities and strategies. Appreciation and trust enables to critically questioning basic and secondary democracy dimensions of quality-indicators and their backgrounds deriving from democracy theory, thus allowing evolvement of a broader understanding of how democracies work (Basic democracy dimensions: freedom, equality, control, sustainable development; secondary democracy dimensions: the rule of law, participation, competition, vertical accountability, horizontal accountability, freedom, equality, responsiveness; Campbell et al. 2015).

Besides future perspective, also the comparative approach from a global perspective of evaluation offers a new, neutral reference system beyond usual fights between right or left wing positions. This is why evaluations going beyond national contexts by offering global views on democracies can initiate curiosity and political system learning.

Instead of "either. . .or" questions, "as well as" answers will occur in processes like, e.g., comparing freedom focused evaluation results of USA to equality driven evaluation results of Europe. Obviously, looking back from sustainable future 2050 to 2020 shows how both, freedom and equality, are crucial for the development of innovation and knowledge systems, representing important parts of advanced democracies.

Global comparisons show that different democracies primarily focus on different dimensions of quality of democracy, producing complementary effects for the overall worldwide development of democracy. Differences between democracies, e.g., like America and Europe, allow democracies to learn mutually from each other (Campbell et al. 2015).

In order to maintain sustainable development of democracies by changing regulations and laws, monitoring corruption, transforming procedures such as increasing application of referendums, or by implementing democratic audits (Campbell and Carayannis 2014), the political system is in need of external impulses for political system learning. Bringing democracies to an advanced level (Campbell et al. 2015) enables societal, economic, and ecological transformations by not only allowing knowledge and innovation flows but also offering an important framework for self-transformation of distinct sectors on system level.

Pluralism and heterogeneity are crucial and decisive for progressing quality of democracy (Campbell et al. 2015). Hence, quality of democracy encourages knowledge and innovation so that quality of democracy and progress of innovation

mutually connect and amplify each in a cross-helix mode and manner. This relates research on quality of democracy to research on innovation (innovation systems) and the knowledge economy (Carayannis and Campbell 2014).

Knowledge and Cyberdemocracy in Need of System Learning

Innovation systems and knowledge democracies go far beyond knowledge-based democracies aiming at transforming the political system and its economic, societal, and ecological context in a sustainable way. This needs transdisciplinary approaches such as participatory foresight processes and Cyberdemocracy approaches.

Forward looking activities and technology assessments as well as ICT-based Cyberdemocracy approaches are both, distinct as well as complementary parts of a knowledge democracy.

Looking at participatory foresight processes within the policy cycle highlights its function for governance as following:

Foresight aims at framing problems by co-creative analysis and mapping as well as at strategic agenda setting by identifying policy targets and implementation paths. In addition, foresight supports informed decision-making and implementation processes with respect to new policy instruments and R&D programs addressing different realms of policy.

Finally yet importantly, foresight is an instrument for long-term orientation of political systems thus initiating sustainable system learning.

Foresight brings longer-term perspectives and broader knowledge bases into decision-making processes, transcending both administrative and epistemic boundaries. Thereby they refer to rules of the game of advanced democracy while shaping them at the same time: pluralism, diversity, and heterogeneity of different knowledge and innovation paradigms in coevolution drive the interaction and relationship of competition, cooperation, and learning processes characterizing democracies at the stage of advanced knowledge systems (Campbell and Carayannis 2014).

Innovation is a systemic phenomenon by nature as it results from the continuing interaction between different actors: Focusing on innovation systems and their functioning we can see that attempts to address innovation system failures and democracy failures demand policy attention to actors, interactions, and institutions.

Actors include a wide range of types of organizations, including firms (large and small, multinational and domestic), universities, public research labs, government ministries and agencies, intermediary bodies, and private consultants. In democracies, where organizations are either missing or weakly developed, a reorientation of innovation systems towards democracy and innovation failures often requires not only the inclusion of stakeholders concerned but also the establishment of new organizations or adaptation of existing ones (Cagnin et al. 2008). Thus, looking forward does not only reflect but also initiate institutional change.

Cooperation and interactive learning are central to the processes of innovation. Such interactions involve firms, universities, government labs, ministries, and funding agencies, among others. Weak interactions often are diagnosed as problems

for innovation systems, since cycles of learning and innovation are less likely (Cagnin et al. 2008).

Institutions constitute the rules of the game and codes of conduct that reduce uncertainty in the innovation system. They are generated by the activities of actors and their interactions with one another and structure these activities and interactions at the same time. (Hard and soft) Institutions provide important levers for policy to shape actors' behavior and interaction (Cagnin et al. 2008).

Participatory foresight processes combine diverse sources of knowledge deriving from a wide range of actors. Building up rooms of trust and reliability, they enable access to the collective, tacit knowledge of experts, decision makers, and civil society. This collective wisdom allows co-creation of desirable futures and identification of good practice stories of how to overcome obstacles or even crises. This enables intensive interactions, mutual learning processes by going beyond usual values and prejudges, and critical questioning blind spots by means of various feedback loops.

This second-order learning allows transformation of daily routines of individuals as well as of systems. Foresight processes allow both individual learning and partial system learning and mobilize huge energy for implementing future-oriented roadmaps and activities: This leads to changed behavior to the effect that policy makers and experts, returning into their professional environment, act as multipliers for change by driving coordinated cross-sectoral and cross-disciplinary solutions inside out of organizations.

Obviously, innovation systems are not only driven by policy measures or foresight processes but also by self-organized activities deriving from ICT-based Cyberdemocracy. Cyberdemocracy, being a part of knowledge democracy, is connected to democracy by building and forming IT-based infrastructures and public spaces, where IT helps in creating new types and new qualities of public space.

Civil society transforms into a media-based and culture-based public thus carrying on and advancing knowledge. In contrast to large group processes of foresight, limited by about 150 people, ICT-based knowledge of Cyberdemocracy allows a quick and global spread of insights and new information beyond local, national, and regional boundaries addressing a global society. This global society regarding global democracy can be translated into niches and systems of intergovernmental cooperation or supranational integration.

Applying criteria of innovation system (actors, interactions, institutions) we can characterize Cyberdemocracy by weak interactions and loose contacts between single actors. This reduces power of system transformation inside out. Nowadays Internet sees both the provision of equal access to crucial information as well as manipulation by the means of incitement to join acts of violence and or lies on certain incidents in the web. This calls for experts as well as a careful governance of virtual knowledge processes as well as for debates on new rights and new freedoms of citizens. Governments are challenged to protect their citizens against manipulations as well as their own demands of monitoring individual movements that are at conflict with principles of quality of democracy (Campbell et al. 2015).

Regarding this dilemma of Cyberdemocracy, participatory forward-looking technology assessments (FTA) could enhance collective decision-making related to the "How" of implementation as well as the "rules of the game" of implemented ICT technologies and applications. Thus, they could help to avoid the enforcement of particular interests deriving from economy or national states: Neither the usage of big data – deduced from permanent tracking of users behavior – for competitive economic advantages in markets nor multiple options of monitoring citizens' or staff-members' behavior in public spaces or firms should be goals of Cyberdemocracy. Thus, forward-looking technology assessments could support political system learning of how to proceed with these new opportunities by maintaining positive effects of IT while in parallel hindering negative impacts on civil society or advanced democracies.

Obviously, we can expect many benefits from Cyberdemocracy such as the widening of an equal access to education, information, and participation. In addition attempts to reinvent innovation or political systems place demands on policies and governance aiming at provoking the development of more transparent and accountable forms of governance able to spread high quality knowledge and continuous flows of knowledge discourses beyond the limits of nation states. Cyberdemocracy would allow co-creation of national, transnational, and in fact global knowledge spaces thus supporting the extension of various advanced democracies on a global level (Campbell and Carayannis 2014). Thus, Cyberdemocracy turns out to be the vision of a global democracy within the meaning of a global society.

References

Argyris, C., & Schön, D. A. (1999). *The learning organization. Basics methods, practice*. (Authorised translation by Wolfgang Rhiel). Klett Cotta: Stuttgart.

Arnold, E. (2004). Evaluating research and innovation policy: A systems world needs systems evaluations. *Research Evaluation, 13*, 3–17.

Bandelow, N. (2009). Politisches Lernen. In N. Bandelow & K. Schubert (Eds.), *Lehrbuch der Politikfeldanalyse 2.0* (pp. 313–347). Munich: Oldenbourg.

Bateson, G. (1988). *Ecology of mind. Collected essays in anthropology, psychiatry, evolution and epistemology* (3rd ed.). Frankfurt/Main: Suhrkamp.

Béland, D., & Cox, R. (2013). The politics of policy paradigms. *Governance, 26*(2), 193–195.

Biegelbauer, P. (2013). *Wie lernt die Politik – Lernen aus Erfahrung in Politik und Verwaltung*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Biegelbauer, P. (2015). How different forms of policy learning influence each other: Case studies from Austrian innovation policy-making. In *Policy studies* (CPOSI 18027). Bangalore/Chennai: Techset Composition India (P), Ltd.

Boden, M., Cagnin, C., Carabias, V., Haegeman, K., & Konnola T. (2010). *Facing the future: Time for the EU to meet global challenges* (EUR 24364 EN). Luxembourg: Publications Office of the European Union. http://ftp.jrc.es/EURdoc/JRC55981.pdf. Accessed Oct 2011.

Cagnin, C., Keenan, M., Johnston, R., Scapolo, F., & Barre, R. (Eds.). (2008). *Future-oriented technology analysis – Strategic intelligence for an innovative economy*. Heidelberg: Springer.

Cagnin, C., Effie Amanatidou, E., & Keenan, M. (2012). Orienting European innovation systems towards grand challenges and the roles that FTA can play. *Science and Public Policy, 39*, 140–152.

Campbell, D. F. J., & Carayannis, E. G. (2014). Explaining and comparing quality of democracy in quadruple helix structures: The quality of democracy in the United States and in Austria, challenges and opportunities for development. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 117–148). New York: Springer. http://link.springer.com/book/10.1007/978-1-4939-1028-1 and http://www.springer.com/de/book/9781493910274.

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493. http://link.springer.com/article/10.1007/s13132-015-0246-7.

Carayannis, E. G., & Campbell, D. F. J. (2014). Developed democracies versus emerging autocracies: Arts, democracy, and innovation in quadruple helix innovation systems. *Journal of Innovation and Entrepreneurship*, *3*. http://www.innovation-entrepreneurship.com/content/pef/s13731-014-0012-2.pdf and http://www.innovation-entrepreneurship.com/content/3/1/12

Depledge, M., Bartonova, A., & Cherp, A. (2010). Responsible and transformative innovation for sustainable societies. Fundamental and applied research. Report of the Environment Advisory Group, Dec 2010. Brussels: European Commission.

Edler, J., & Kuhlmann, S. (2008). Co-ordination within fragmentation. Governance in knowledge policy in the German federal system. *Science and Public Policy, 35*(4), 265–276.

Erickson, M. H. (1954). Pseudo-orientation in time as a hypnotherapeutic procedure. *Journal of Clinical and Experimental Hypnosis, 2*. German. (1998). Pseudoorientierung in der Zeit als hypnotherapeutische Vorgehensweise. In E. L. Rossi (Ed.), *Gesammelte Schriften von Milton H. Erickson. Band VI, Innovative Hypnotherapie II*. Heidelberg: Publ. Carl-Auer.

Eriksson, E. A., & Weber, M. (2008). Adaptive foresight: Navigating the complex landscape of policy strategies. *Technological Forecasting and Social Change, 75*, 462–484, AIT Austrian Institute of Technology.

Evans, J., Jones, R., Karvonen, A., Millard, L., & Wendler, J. (2015). Living labs and co-production: University campuses as platforms for sustainability science. *Journal Elsevier: Current Opinion in Environmental Sustainability, 16*, 1–6. www.sciencedirect.com.

Freeman, E. (1970). Stakeholder theory of the modern corporation. In M. Hoffman, R. E. Frederick, & M. S. Schwartz (Eds.), *Business ethics – Readings and cases in corporate morality* (4th ed.). New York: McGraw-Hill.

Freeman, R. (2006). Learning in public policy. In R. E. Goodin, M. Moran, & M. Rein (Eds.), *The Oxford handbook of public policy*. Oxford: Oxford University Press.

Georghiou, L., Harper, J. C., Keenan, M., Miles, H., & Popper, R. (Eds.). (2003). *The handbook of technology foresight: Concepts and practice*. Northampton: Edward Elgar Publishing.

Hall, P. (1993). Policy paradigms, social learning, and the state. *Comparative Politics, 25*(39), 275–296.

Hall, P., & Taylor, R. C. R. (1996). Political science and the three new institutionalisms. *Political Studies, 44*(5), 936–957.

Hargreaves Heap, S. P., & Varoufakis, Y. (2004). *Game theory. A critical text*. London: Routledge.

Holste, D., Kubeczko, K., Schartinger, D., Helmreich, S., & Wilhelmer, D. (2010) A complementary architecture to build foresight. In K. R. E Huizingh, S. Conn, M. Torkkeli, & I. Bitran (Eds.), *Proceedings of The XXI ISPIM conference, June, 6th–9th, Bilbao*, CD-ROM, ISBN 978-952-214-926-8.

Hustedt, T., & Veit, S. (2014). Forschungsperspektiven auf Regierungs- und Verwaltungskoordination: Koordinationsprobleme und Erklärungsfaktoren. *der moderne staat, 7*(1), 17–36.

Hüther, G. (2010). *Die Macht der inneren Bilder. Wie Visionen das Gehirn, den Menschen und die Welt verändern* (6th ed.). Göttingen: Vandenhoeck & Ruprecht Verlag GmbH & Co KG (2004, 2010).

Huxham, C. (2010). Theorizing collaboration practice. *Public Management Review, 5*(3), 401–423.

Koch, C. (2008). The super ministry approach: Integrated governance of science, technology and innovation with contracted autonomy. *Science and Public Policy, 35*(4), 253–264.
Laegreid, P., Sarapuu, K., et al. (2015). New coordination challenges in the welfare state. *Public Management Review, 17*(7), 927–939.
Lindner, R. (2012). Cross-sectoral coordination of STI-policies: Governance principles to bridge policy-fragmentation. In *Innovation system revisited: Experiences from 40 years of Fraunhofer ISI research* (pp. 275–289). Stuttgart: Fraunhofer Verlag.
March, J. G., & Olsen, J. P. (1989). *Rediscovering institutions*. New York: Free Press.
Markowitsch, H. J. (2013). A paradigm shift is needed! In M. Eckoldt (Ed.), *Can the brain understand the brain? Dialogues about brain research and the limits of perception and insights* (pp. 25–28). Heidelberg: Publ. Carl-Auer Systeme.
Mayntz, R. (1980). *Implementation of policy programs. Empirical research report*. Königstein: Athenäum.
Miles, I. (2002). *Appraisal of alternative methods and procedures for producing regional foresight*. Report prepared by CRIC for the European Commission's DG Research funded STRATA-ETAN Expert Group Action. Manchester: CRIC.
Miles, I. (2003). Foresight methodology. In L. Georghiou, J. C. Harper, M. Keenan, I. Miles, & R. Popper (Eds.), *The handbook of technology foresight: Concepts and practice*. Northampton: Edward Elgar Publishing.
Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. *Academy of Management Review, 22*(4), 853–886.
Nowotny, H., Scott, P., & Gibbons, M. (2003). Mode 2 revisited: The new production of knowledge. *Minerva, 41*, 179–194.
Oliver, M., & Pemberton, H. (2004). Learning and change in 20th-century British economy policy. *Governance, 17*(3), 415–441.
Peters, G. B. (Ed.). (1996). *Lessons from experience: Experimental learning and administrative reform in eight democracies*. Oslo: Scandinavian University Press.
Peters, G. B. (1998). *Managing horizontal government: The politics of coordination*. Research Paper, Canadian Centre for Management Development.
Peters, B. G. (2013). Toward policy coordination: Alternatives to hierarchy. *Policy & Politics, 41*(4), 569–584.
Popper, R. (2008). Foresight methodology. In L. Georghious, J. Cassingena Harper, M. Keenan, I. Miles, & P. R. Edward (Eds.), *The handbook of technology foresight, concepts and practice*. Edward Elgar Publishing.
Popper, R., Keenan, M., Miles, I., Butter, M., & Sainz, G. (2007). *Global foresight outlook 2007: Mapping foresight in Europe and the rest of the world*. Manchester: The University of Manchester/TNO.
Rittel, H., & Weber, M. (1973). Dilemmas in a general theory- of planning. *Policy Sciences, 4*, 155–169.
Schein, E. H. (2010). *Organizational culture and leadership* (4th ed.). San Francisco: Jossey-Bass.
Schmidt, G. (2004). Love-affairs betwixt problems and solutions. Hypnosystemic work in difficult contexts. Publ. Carl-Auer-System, Heidelberg, S. 47.
Schofield, J. (2004). A model of learned implementation. *Public Administration*, *82*(2).
Senge, P. M., et al. (2011). *The necessary revolution. How people and organisations cooperate aiming at co-creation of a sustainable world*. Heidelberg: Publ. Carl-Auer.
Smith, K. (2000). *What is the "knowledge economy"? Knowledge-intensive industries and distributed knowledge bases*. Paper prepared as part of the project 'Innovation policy in a knowledge-based economy' commissioned by the European Commission. Available at http://www.druid.dk/uploads/tx_picturedb/ds2000-123.pdf. Accessed Aug 2007.
Verhoest, K., Bouckaert, G., et al. (2007). Janus-faced reorganization: Specialization and coordination in four OECD countries in the period 1980-2005. *International Review of Administrative Sciences, 73*(3), 325–348.

Voets, J., Verhoest, K., et al. (2015). Coordinating for integrated youth care: The need for smart metagovernance. *Public Management Review, 17*(7), 981–1001.

Wagenaar, H. (2004). "Knowing" the rules: Administrative work as practice. *Public Administration Review, 64*(6), 643–655.

Wilhelmer, D. (2009). *Reminiscence of a better future. Syntax for a complementary innovation counselling*. Heidelberg: Publ. Carl-Auer-System. ISBN 978-3-89670-913-4.

Wilhelmer, D. (2012). Komplementärer foresight. Ein neuartiges Instrument zum Steuern von Open Innovation Prozessen. S. 8. In I. Serhan (Hrsg.), *Innovation Exzellenz: Wie Unternehmen ihre Innovationskraft systematisch steigern*. Düsseldorf: Symposion Publishing. Erscheinungsdatum Jänner 2012. ISBN 978-3-86329-425-0.

Wilhelmer, D. (2013). Zukunft entsteht in Co-Kreation. Zeitschrift ChangeX – Folge 25 der Serie Zukunft der Zukunft, 4, 12. Dezember 2013, S. 3.

Wilhelmer, D., & Erler, H. (2010). Swarovski: Mit Netzwerken Innovationsprozesse steuern. In: Open Innovation. Symposion Verlag 2010. In I. Serhan (Hrsg.), *Open Innovation umsetzen. Prozesse, Methoden, Systeme, Kultur*. Düsseldorf: Symposion Publishing. ISBN 978-3-939707-75–2.

Wilhelmer, D., & Nagel, R. (2013). *FORESIGHT – Ein Managementhandbuch für das Gestalten von Open Innovation*. Heidelberg: Carl Auer Verlag. ISBN 978-3-8497-0011-9.

Willke, H. (1998). *Systemisches Wissensmanagement*. Stuttgart: Lucius und Lucius.

Willke, H. (2004). *Einführung in das systemische Wissensmanagement* (p. 60). Heidelberg: Carl Auer Systeme Verlag.

Woolthuis, R. K., Lankhuizen, M., & Gilsing, V. (2005). A system failure framework for innovation policy design. *Technovation, 25*, 609–619.

Concept for Strategic Foresight Knowledge Development Framework for Horizon Scanning Center

11

Joachim Klerx, Johannes Göllner, Christian Meurers, and Klaus Mak

Contents

Abstract

Big data analytics, predictive analytics, and artificial intelligence can contribute to improve the predictive power of risk models. In a world of increasing complexity and interdependency, the ability to capture access and utilize big data sets will

J. Klerx (✉)
Foresight, Research, Technology and Innovation Policy, Austrian Institute of Technology, Vienna, Austria
e-mail: joachim.klerx@ait.ac.at

J. Göllner
Institute of Strategy, Foresight, Risk and Innovation Management, MASARYK University, Socio-Economic Faculty, Brno, Czech Republic

Center for Risk and Crisis Management, University of Natural Resources and Life Sciences, Vienna, Austria
e-mail: johannes.goellner@bmlvs.gv.at

C. Meurers · K. Mak
National Defence Academy, Ministry of Defence and Sports, Republic of Austria, Vienna, Austria
e-mail: christian.meurers@bmlvs.gv.at; klaus.mak@bmlvs.gv.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_36

determine success in risk management. In this publication, a framework for knowledge management of Horizon Scanning Centers (HSC) is proposed to improve the effectiveness of these centers, by using new methods of big data analytics. After discussing foresight as trigger for changes, with epistemic foundations and information logistics, a framework for knowledge performance and risk analysis is presented. This framework is designed to improve the effectiveness of HSC and thus to improve the governance of uncertainty in the age of big data.

Keywords
Governance of uncertainty · Big data · OSINT · Knowledge development · Foresight · Horizon scanning · Z-model · Information logistics · Knowledge performance systems

Introduction

Dealing with zettabyte of data will lead to completely new approaches in the governance of uncertainty. The well-known four "V"s of big data (volume, variety, velocity, and veracity) (IBM 2016) are by no means the only issue of big data, relevant for risk analysis. In particular, the very high amount of available attributes in analytics and the increasing amount of correlated and interdependent variables should lead to more demanding models, but finally to much better insights for risk analysis.

Big data analytics, predictive analytics, and artificial intelligence can contribute to these analytical approaches. They can improve the predictive power of risk models, exponentially improve system response times and effectiveness, provide more extensive risk coverage, and generate significant cost savings. In a world of increasing complexity and interdependency, the ability to capture, access, and utilize big data sets will determine success in risk management.

The combination of OSINT analytics, topic mining, emotion mining, and strategic foresight analytics can give an operational framework for big data analytics in risk management (Palomino 2013a).

In recent decades, a number of more or less elaborate foresight studies were conducted in order to obtain reliable information about what the future holds. In these studies, expectations are worked out and scientifically reasoned what could and what could not happen in the future. This knowledge may change quickly and less quickly depending on current events.

The organizational units which are responsible for long-term planning are increasingly establishing processes for continuous monitoring to improve the effectivity of foresight processes. This "low-level horizon scanning" is helpful to respond to unforeseen structural changes, effected by the long-term planning.

In this publication, a framework for knowledge management of Horizon Scanning Centers (HSC) is proposed to improve the effectiveness of these centers, by using new methods of big data analytics. After discussing foresight as trigger for changes, with epistemic foundations and information logistics, a framework for knowledge performance and risk analysis is presented. This framework is designed

to improve the effectiveness of HSC. The framework for knowledge development will focus on the combination of information logistics and risk analysis in a big data context. Finally, an outlook on future governance of uncertainty is given to discuss existing solutions in view of future developments.

Management of Horizon Scanning Center

It is a well-known phenomenon in change management that new pattern of behavior do not always go along with an undivided joy for change. This tendency to persist in a given situation is supported by a perception filter to avoid cognitive dissonance. Every perception about future developments is influenced by an expectation context, built upon previous experience, filtered by the senses, the mind, the group pressure, and the emotional well-being.

Organizational changes and innovations can trigger fear (social innovations can even trigger riots) or other forms of bad emotions. Foresight processes sometimes produce future expectations, which do not fit into the actual common worldview. These results have the potential to lead to considerable debates. To overcome this, a profound support by big data analytics with fact prove is helpful.

In recent years, first Horizon Scanning Centers (HSC) emerged with high performance data mining and other forward-looking activities as method to identify weak signal (Amanatidou et al. 2012) for future developments and disruptive events. By quantitative evaluation of analytical results from different sources, it is possible to improve the reliability from foresight processes and thus to support the strategic long-term planning with more reliable future expectations.

The management concept for a typical Horizon Scanning Center built upon the structure of a typical knowledge-intensive organization consists of core processes (environment analysis, horizon scanning, and relevance-based content) and support processes (knowledge management, risk management, ICT support, risk management, and public relations). These management processes needs to be adapted to the methods of big data analytics. The risk management in particular, however, is not only a support process. As all future expectations are more or less likely expectations that are realized with a certain probability, risk assessments are considered as a core analytical approach in HSC with strategic relevance, as explained later. For the HSC, this is a strategic planning and management process. HSC as a specific center or as integral part of the strategic management department have proven to be very effective in the business environment.

It is a well-known problem in the business environment that market leader within a disappearing market, maybe because of a disruptive technical innovation, remains remarkably often too long in their processes (as Kodak with analogue films at the time of digital cameras and Nokia at the time of smart phones).

For a commercial organization, it is not sufficient to just prepare for structural change, when they are ongoing. It is rather important to anticipate changes in advanced. For this, it is necessary that a majority of employees, especially the

employees with management responsibilities, understand not only those changes, but jointly develop strategies for anticipating these changes.

Since this organization-wide process needs a remarkable time in larger organization, it is a matter and culture of communication to set up and improve this process. Early detection system and proper knowledge and innovation management are supporting this.

Foresight studies can help but are often too rare to ensure reactions in time. The time interval between individual large-scale foresight studies can be 5 and 10 years. A resource-efficient solution for this would be a continuous horizon scanning performed with low resources level, either by a department or by an outsourced independent organization.

Foresight as Trigger of Changes

For about a decade, foresight studies have been used successfully in long-term planning. These are used in relatively large intervals usually for an entire domain of knowledge (Trawinska-Konador et al. 2015), such as security policy or transport planning; studies made summarize the current expectations of the future development. Assuming a formal foresight starts at the time t_0, this process will produce expectation valid for t_1. Suppose the next foresight is provided at time t_6, with a time horizon to t_7.

Then it may very likely happen that a surprising event at time t_2 leads to a system breakdown, which could have been avoided by timely planning. In this situation, it takes time to start a new foresight (t_4-t_5), which means that for a certain period, decisions are made without proper foresight knowledge. This knowledge should be produced in a quality-assured process from an HSC (not to mention the fact that large organizations get problems with structural changes, even when they have proper knowledge and enough resources) (Fig. 1).

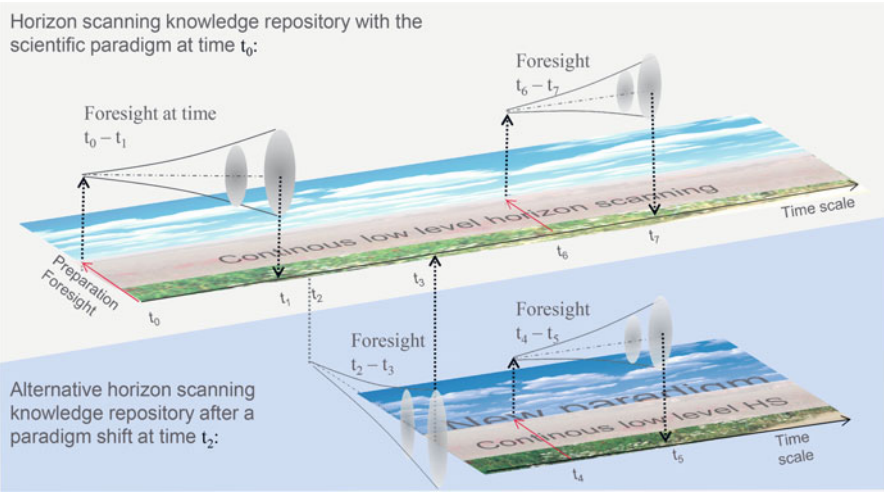


Fig. 1 Relationship of foresight and Horizon Scanning Center (Klerx 2012)

In an HSC, it is better to foresee the system broken in a continuous process, as soon as the first signs are visible would. Then, a foresight process could, in the shortest possible distance to t_2, start that accompanies the structural change, and the next foresight (t_4-t_5) then takes place already under a new paradigm.

Epistemological Foundations of Foresight

Although the term foresight was already introduced around 1932 by H.G Wells in the context of future research, the term was used in a specific meaning in Europe in the last decade. In the last time, there has been a whole series of foresight projects in Europe, which have had the aim of supporting long-term planning in the EU. In particular, the European Commission has established working groups that take and share the results from these often EU-funded projects. The Institute for Prospective Technological Studies of the European Commission (IPTS) has developed a handbook (ForLearn) in which the methodological experience of this time is summarized. This guide is currently maintained and occasionally revised by the Austrian Institute of Technology, on the European Foresight Platform (EFP 2016).

As Kreibich mentioned (Kreibich 2009), the modern future research assumes that the future is not in principle completely determined and that various future developments (futures) are possible and formable. The typical foresight process, as shown in Fig. 2, includes these typical design elements.

Depending on the use of specific intention and methods, foresight processes can produce different types of knowledge. Each result of a foresight project is concrete knowledge product, either, e.g., an opinion, a conjecture, a speculation, an ideology, or the expression of an attitude of faith. Even false knowledge is a valid knowledge

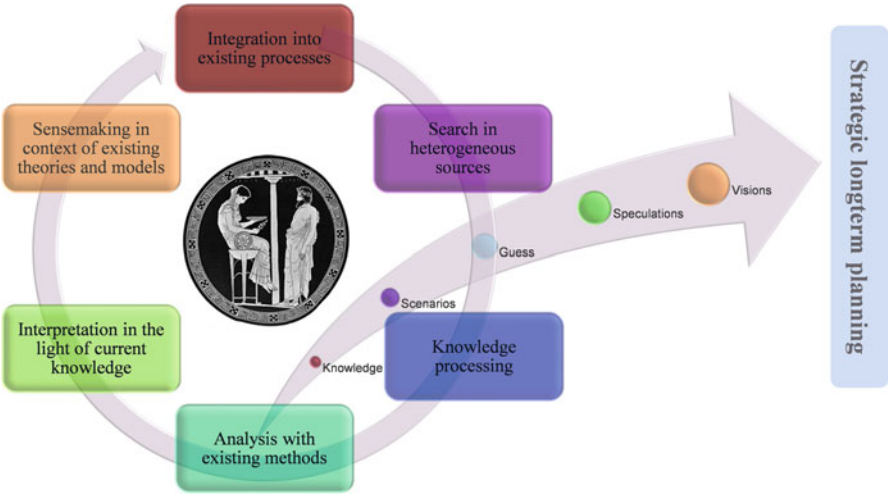


Fig. 2 Processes and results of a typical foresight project (Klerx 2015)

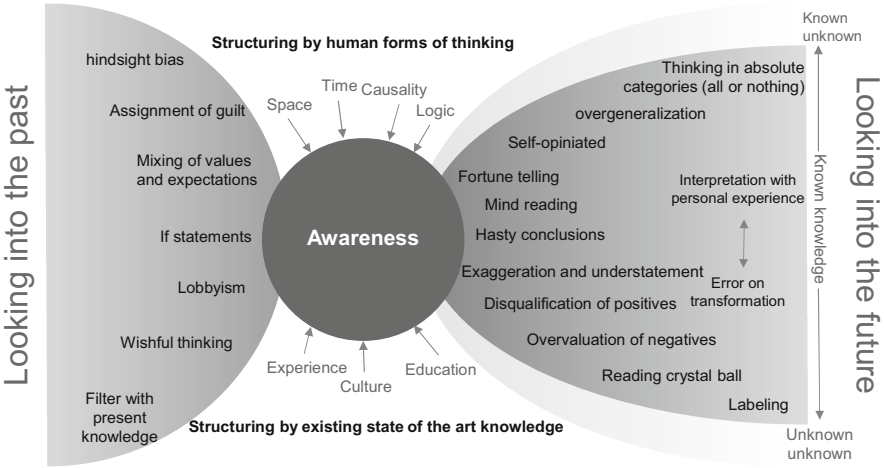


Fig. 3 Cognitive distortions in foresight processes (Klerx 2015)

product in the foresight process. In particular, false knowledge, ignorance, and ideologies provide starting points for processing creative and participative processes. The more creative methods work better when they are not judged too early and too fast. In this case, possible additional results are left untouched. Fig. 3 shows all different cognitive distortions, which tend to happen in foresight workshops.

Typical cognitive distortions, in a foresight process, are based on false knowledge for different reasons. This to say, specific sources of knowledge are known as a source of false information. Knowledge in the context of personal experience, culture, or education might be wrong, because it was never checked against empirical results. In particular, visions, ideologies, and beliefs tend to form limitations in the variance to acclaimed strategies. In general, expectations are structured, based on external forms, such as time, space, causality, and logic. These forms can cause distortion of both knowledge from past experience and knowledge about future expectations, as all this knowledge relies on logical causes. However, disruptive events, unconventional solutions, and other surprises might be outside of the common logic.

The cognitive distortions in foresight processes arise primarily from the fact that knowledge of the future is always incomplete and that foresight results almost always include different forms of ignorance. Knowing about these different forms of possible ignorance can improve the reliability of the knowledge development process. However, for this, a very high standard in the epistemological foundations is necessary. Thus, dealing with risk and insecurity is in the methodical focus of HSC.

The human mind has a range of different strategies to deal with incomplete knowledge. The use of some of these strategies are helpful in foresight processes, others are not. It is therefore a central task in foresight processes, to develop methods to deal with ignorance of different types, and promote constructive and successful ways to deal with these different types of uncertainty.

The cognitive distortions about future expectations include both hasty conclusions as well as the tendency to see in streams patterns, even if none is there. The "nonclinical" forms of apophenia, clustering illusion, and pareidolia are forms of complexity reduction, which actually should contribute to "overload protection." In foresight activities, it is always necessary to decide whether more research and analysis are necessary, or whether the findings for a reliable expectation of formation are sufficient. Even if the resources are scarce, an adequate protection of the expectations for the future should not be left out, because the quality assurance contributes to the reliability.

This shows that the automatic scanning of HSC needs to be accompanied by sophisticated knowledge development mechanism. These should be set up in a self-learning environment to improve the HSC processes iteratively over time.

Information Logistics

This approach of continuously monitoring relevant sources is not fundamentally new. However, since a process of continuous monitoring can easily become quite expensive, there are in most existing Horizon Scanning Center's efforts to automate this process.

About the methods of automation, the active use of latest knowledge management tools and the combination with risk management methods are success for Horizon Scanning Center (HSC). Horizon scanning can provide a wide variety of information. According to the purpose of the HSC, it is possible not to overlook any systematical gaps and to detect those as early as possible. In particular, searching for weak signals of all knowledge products can be a challenge.

Having in mind that the HSC should contribute to strategic long-term planning, it is clear that the early discovery of disruptive events and any other knowledge product of an HSC is essential as to be on top on the methods to deal with uncertainty. Identified system gaps are delivered with success if all processes of an HSC are organized so that they will get better over time.

Figure 4 shows the different kinds of knowledge products in a Horizon Scanning Center (HSC) as a collection of processes of knowledge accumulation with quality assurance and risk assessment evaluation (Z model). The knowledge development process of an HSC starts with information logistics processes (Dinter and Winter 2008) for data acquisition and information retrieval. This usually includes big data capabilities for automatic weak signal mining. In a second step, the quality of the information is enriched by human analytics and crowd intelligence.

The enrichment process uses general and domain-specific knowledge type classifications to create in a first step a collection of scenarios for situational awareness, based on available information. Plausible and resilient scenarios are created by using background information and additional knowledge from experts. This leads in a second step to a situational awareness picture, based on existing knowledge about possible scenarios. Finally, the risk assessment of these scenarios leads to a multi-dimensional picture of threats (Powell et al. 2016) and opportunities of the future.

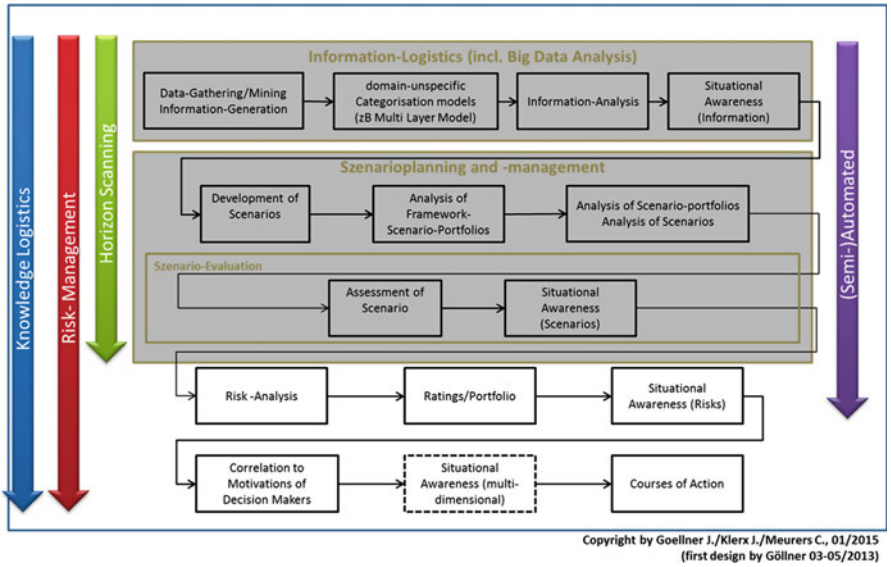


Fig. 4 Knowledge logistics in a Horizon Scanning Center (Göllner and Klerx 2013)

This serves as strategic knowledge for long-term planning and decision making in organizations with adaptive innovation management.

Following the knowledge development model, "Z-model," it is possible to establish proper organizational capabilities to set up an HSC. The Z-model deals with different challenges of modern information logistics with respect to the risk management. The scope of this model is the generation of situational awareness from an information perspective. Therefore, the model defines a process to gather, categorize, and analyze information from big unstructured data sets and integrate this into a situational picture. To be able to deal with the growing amount of information and its increasing heterogeneity, modern organizations have to cope not only with new technologies, methodologies, management approaches, and processes but with the development and integration of new infrastructures and information management as well as logistic concepts (Meurers et al. 2015).

Information logistic can be seen as a part of information management and is a fundamental basis and a backbone for the development and the control of organizations. It is an important part of a continuous organizational development process and has to be adapted and optimized permanently, following the emerging challenges and requirements of a highly dynamical, rapidly changing, and complex environment.

To have access to the right information in the right time at the right place (McNurlin and Sprague 2002) is the fundamental basis for all management tasks on all levels of an organization and guarantees the ability for development of and innovation in an organization. Hence, modern information logistics has to follow a generic approach in process design, which considers the integration of

organizational requirements, regulations by law (Göllner et al. 2015; Forst 2014), technical structures, and security issues in regard to stay highly dynamic and adaptable.

The mechanism of the knowledge development model "Z-Model" creates an information logistics basis for all further tasks of organization development, leading, and regulation. It has a significant importance in most company sectors and forms the backbone of an organization. Only those who are able to continuously adapt its information logistics to the specific challenges and tasks of a constantly and ever more rapidly changing world will stay successful in the future.

The highly dynamic evolution in the fields of information, communication, technology, and data puts companies in increasingly shorter development cycles in front of growing challenges. Modern organizations must nowadays deal not only with new technologies, methods, management approaches, processes, or business units, but also require an appropriate infrastructure and information logistics in the background. Only when information at the right time in the right amount reaches the correct destination, the leading and management ability of the organization is ensured. Information logistics is therefore beyond all technological developments, the need of the hour, as it ensures the basis for all activities of an organization (Dinter and Winter 2008).

The aim is to combine new techniques and approaches with conventional methods to generate the best possible situational awareness and future expectations with measurable strategic value.

In the environment of the Austrian Ministry of Defence and Sports, new challenges for the organization emerge daily. Numerous research projects are dealing with new approaches and solutions in, for example, the areas of risk management, knowledge development and management, crisis and disaster management, and operations research, which apart from models and methods often produce important technical developments for the organization.

The main challenge of modern information logistics is the timely provision of correct, as complete as possible, and appropriately preprocessed information to the target audience at the right time at the right place. Following the rapid technological change, these challenges can be achieved by a purely technical point of view today. An essential prerequisite for the effective use of new technologies is the transformation into an information and knowledge-based organization, which is able to utilize the information provided in the analysis, assessment, and planning stages. Every participant in the processes must therefore be able to obtain the necessary perspectives on the existing data to carry out their work.

Information retrieval, information provision, and information processing are those core components upon which all forms of information logistics are built on. They are vital for ensuring the information logistics chain. This chain in turn is a precondition that an organization continue to function in an information- and knowledge-based world. Even military capabilities that have been developed over centuries are affected radically by the change in information logistics. Only when the necessary information and its associated analysis and processing systems are available, crisis and conflict situations can be decided correctly and in time. Additionally,

the possibility of networking (Shi and Zhu 2013) with the information systems of other partners, particularly in assistance missions and in international assignments, is of increasing importance in this context.

Trends and developments like big data (Mayr-Schönberger and Cukier 2013), open source intelligence, ubiquitous information systems, and military information modeling have created a situation, in which the governance of uncertainty is supported by the establishment of necessary processes for the sustainment of the organization's ability to decide and act. In order to implement the processes of information logistics legally and reliably, information security and privacy must be in the focus of consideration.

The challenge of a modern information logistics is therefore the development and implementation of a comprehensive and integrative approach, which considers the legal framework, the organizational requirements for the working environment, and the technical, in particular the safety developments, as well as the technological impacts, early in process design.

In particular, for the Austrian Armed Forces and the superior Ministry of Defence and Sports, this field offers great opportunities to become not only more efficient and effective, but to enhance the performance of being security organization of the Republic of Austria in common.

An Architecture for a Knowledge Development Framework

The proposed architecture for a knowledge development framework (Pavlic et al. 2015) for HSC is built on top of the Z-model and increases the effectiveness by using knowledge performance modeling and risk assessment (Koivisto et al. 2009) to deal with the inherent uncertainty of future developments.

According to the core objectives of a Horizon Scanning Centre (HSC) to prepare relevant knowledge to support strategic long-term planning, the core processes of an HSC consist of an interconnected environment analysis and automated low-level horizon scanning. The "low-level" horizon scanning has significantly reduced expenditure of resources, in comparison to a conventional horizon scanning. In addition, this low-level horizon scanning is designed as continuous process for relevant content scanning in very large scale unstructured datasets.

The core processes of the HSC are supported by a suitable ICT infrastructure, by a documentation system, knowledge management, and overall management. In addition, the core processes (Salzano et al. 2016) involved in management structures that specifically have the knowledge management and risk management is the focus, as shown in Fig. 5.

The core processes focus on the objective of the HSC and serve to meet the information needs of owners and stakeholders as possible.

The environmental analysis is used to understand the system dynamics of the environment and to model so that the consequences of individual information can be estimated as soon as possible from the low-level horizon scanning. A mix of methods of social network analysis, material flow analyzes, time series analysis for

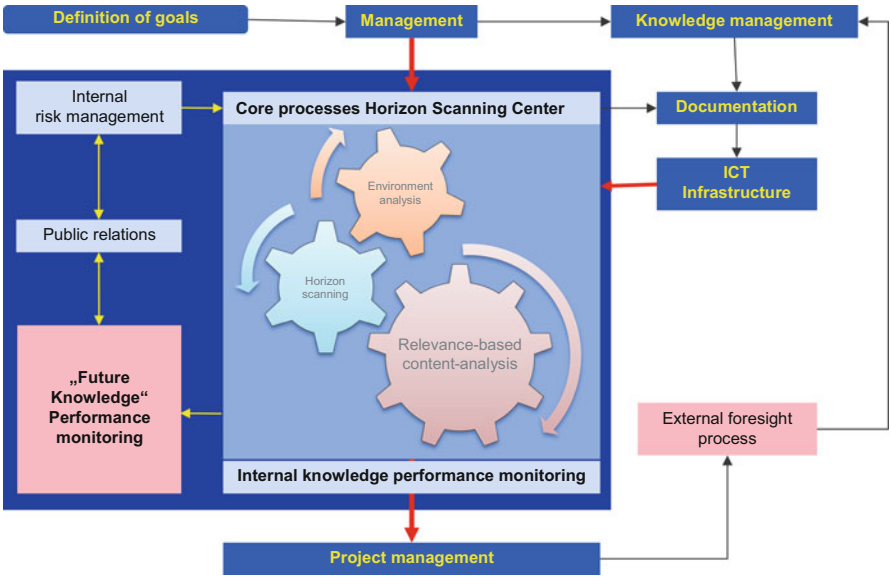


Fig. 5 Process diagram of a situation center for strategic resource analysis (Source: AIT, Innovation Systems, Joachim Klerx)

forecasting of trends by trend extrapolation, and system dynamics modeling have proven to be promising. The data for this mix of methods are available in principle and, however, can require the expenditure of a significant amount of data retrieval. To minimize these costs, strategic partnerships may be helpful.

Automated low-level horizon scanning used methods of text mining as metadata extraction, automated translation, automated author detection, topic mining, and emotion mining to search in the respective selected or identified sources for relevant content. Therefore, a cloud infrastructure is necessary for the ICT infrastructure, which must be dimensioned as a function of the observed sources. Experience shows that require around 10 million sources, a number of 100 nodes in the cloud. With the relevance-based content analysis, the results from the automated scanning verify. In a global scanning, such linguistic skills are necessary to evaluate the respective sources.

According to Fig. 5, different support processes for the operation of an HSC are necessary in addition to the core processes. The main support processes are knowledge management, documentation, and the already mentioned ICT services. In each single day of operation the HSC, a plethora of knowledge and information needs to be processed and stored in the HSC. Thus knowledge management, and documentation are critical processes of the HSC, that must provide long-term learning capabilities for the center. The accumulated knowledge must be saved and documented in a form that allows a gradual improvement in the process. This increases the flexibility and ensures the efficiency of core processes.

In addition to the efficient provision of infrastructure and organization, typical management services must be built and established. In knowledge-intensive organizations such as the HSC, a particular form of risk management is necessary. The risk is usually to generate knowledge not in hazardous substances and equipment, but the possibility of "false." As shown below, for epistemiological reasons, reliable knowledge about the future is not possible. All knowledge products of the HSC are affected by this limitations. Because of this, all different sorts of uncertainty are important knowledge products and needs to be handled properly within the knowledge management of the center. Various statements of the HSC will be subject to different, but usually unknown, uncertainties. Over time, it is therefore necessary to learn from the mistakes of the past and gradually to make reliable statements about the future. Risk management is not only a necessary measure of management, but should be an integral part of the HSC.

The same applies to public relations, one of the central HSC management services. In addition to this, the communication of all public affairs of the HSC is considered as core process and must adequately inform stakeholders and the wider public timely with relevant information. For this, regular and trustfull relationships to local journalists are as relevant as the intense use of social media to comunicate to the stakeholder.

Finally, both the core processes and the supporting processes have to be organized and managed. This management tasks include all organizational tasks such as workflow management, quality assurance, acquisition, and accounting/cost accounting.

To improve over time, it is very important to monitor and evaluate the results against the HSC objective and to improve wherever a performance issue becomes evident. The performance monitoring is necessary for internal knowledge-intensive processes and for the core processes, which produce external knowledge about the future.

Internal Knowledge Performance Monitoring

The first challenge of measuring intellectual capital is to identify knowledge in such a form that it can be assessed. For this, knowledge needs to be referenced to a certain goal. The main goal of the HSC is to identify knowledge of any kind to improve the process to generate knowledge about future developments.

The knowledge performance monitoring (KPM) approach (Göllner et al. 2010) identifies three basic types of knowledge products:

1. service products, e.g., implicit knowledge for implicit usage like an expert, trainer, etc.
2. information products, including explicit knowledge for implicit usage like books, magazines, and other forms of publications
3. software applications, which transform explicit knowledge into a system which is usable even for nonexperts.

The definition of the "knowledge product" and the identification of service products, information products, and software applications enable the HSC to specify the knowledge in a consumable way. The assumption that only consumable and hence applicable knowledge is of interest is a restriction that is acceptable for the assessment of internal processes. However for creating knowledge about the future, the core competence of the HSC, this focus on applicable knowledge is somehow limited. Thus methods to deal with non applicable knowledge should be developed in the HSC.

Based on this, the proposed KPM approach for HSC follows a digitalized balanced scorecard system. The generic structure of the knowledge scorecards is defined as follows:

- *Product perspective:* Goals, indicators, and measures for the actual knowledge products provided by the HSC
- *Processes and structure perspective:* Goals, indicators, and measures in relation to processes executed are used to create the knowledge products (build on top of the already defined core processes, supporting processes and management processes for HSC)
- *Human capital, relations, and competences perspective:* Goals, indicators, and measures of human capital and competences required to create the knowledge products.
- *Resources and support perspective:* Goals, indicators, and measures of budget, infrastructure, material, and tools (including structural capital) as well as information access, which is a basic resource for the HSC

The four perspectives have been derived by analyzing available measurement criteria and validating them against existing experience in the management of an HSC for cyber security. These perspectives have been evaluated according to their applicability to increase the performance of HSC. Based on previous results from Göllner et al. (2010), the perspectives were extend with vertical pillars to provide an architecture for realizing the digital knowledge scorecards.

Figure 6 depicts the developed architecture for the HSC knowledge scorecards. Starting point was the knowledge products that need to be produced, disseminated, and continuously improved through the core processes. The presented three pillars are analyzed according their impact, their management processes, the available versus required skills, and the available versus required input. This matrix has partly been used as a guideline to identify the critical success factors, the knowledge goals, and measurement criteria for internal knowledge monitoring.

In addition to the internal knowledge performance monitoring, HSC as knowledge-intensive organization needs to have a knowledge performance monitoring for the knowledge, created by the core processes and evaluate the results with respect to real future developments. This will be presented in the next chapter.

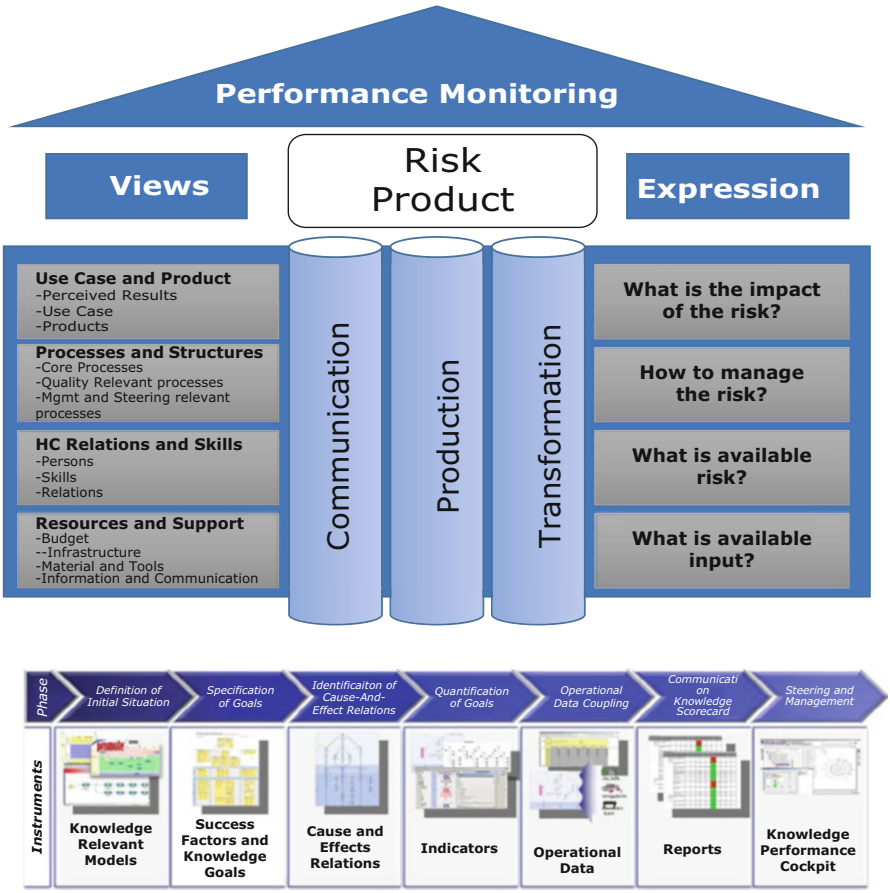


Fig. 6 Overview of the approach for internal knowledge performance monitoring for HSC (Göllner et al. 2010)

"Future Knowledge" – Knowledge Performance Monitoring

As mentioned before, future knowledge consist of very different knowledge products, like threats, social needs, trends, disruptive innovations, events, weak signals, black swans, and others. These knowledge products are notoriously uncertain in the future. Thus, every analytical solution, every visualization of results, and every performance monitoring will have to pay attention to the uncertainty of the grounding knowledge (Konnola et al. 2012).

Typical results from the core processes are structured along a time scale, geographical scales (Mokrech et al. 2012), network distribution, or systems simulation. To create a reliable situational awareness, it is very important to learn from past results. Thus, performance monitoring should focus on the prediction results of previous analytical results and their correlation to present developments.

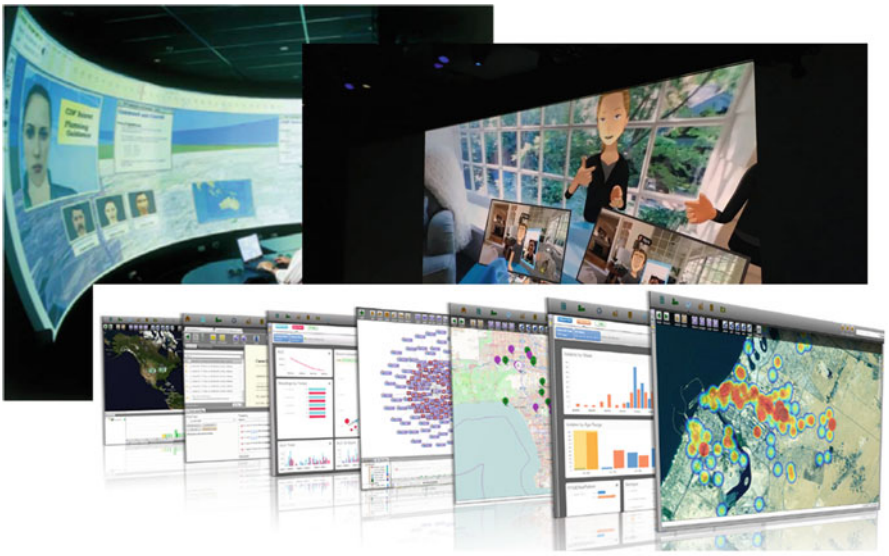


Fig. 7 Visualization of results from core HSC processes

In Fig. 7, some examples from a situational awareness center, analytical software, and 3D environments are shown. 3D environments from simulated or augmented reality in particular will become a meaningful instrument in the future to visualize future scenarios for validation in stakeholder processes. Situational awareness simulations for future scenarios can be used to monitoring the validity and the reliability of future scenarios and their relations to each other.

Scenarios about the future are essentially uncertain. Thus, for each scenario and for the scenario portfolios, a proper risk assessment and prioritization is important (Garnett et al. 2016). For monitoring purpose, the correlation between risk and knowledge products is essential. Each knowledge product needs to be valued with a risk factor and an impact factor. Even if it is notoriously difficult to quantify scenarios about the future, for monitoring and evaluation this step is essential. A collaborative review can improve the monitoring approach (Sutherland et al. 2012).

The monitoring results from all future knowledge generated in the HSC core processes form options for the strategic, operational, and tactical management of organizations in the domain of the HSC (Uusitalo et al. 2009). They are the basis for innovative product developments and strategic human resources capability development. In addition to this, they can be used for adaptive innovation management and innovation management in large-scale innovation networks (Dolinska 2015).

The results can contribute to understand the integration of the digitalization in production, in the supply chain or in the steps to globalization. The structured and organised knowledge logistics of HSC with epistemiological backing will help to

understanding the impact of Enterprise 4.0 and the implications of new digital infrastructures, e.g., cryptocurrencies, like Ethereum and Bitcoin.

For future challenges of integrated supply chain management (Polemi and Kotzanikolaou 2015), the results can contribute with risk analysis, in particular, of complex interdependent risks and with knowledge sharing in teams (Ghobadi 2015), e.g., in dynamic supply chain processes to build up large-scale innovative communities (Dolinska 2015).

Future Governance of Uncertainty

In the future, with climate change in place, new media in place, digitalization, globalization, increasing world population and new forms of communication it is expected, that the amount of interdependent complex risks are increasing. Cyber physical systems, internet of things (IoT), physical internet, IPv6, semantic web applications, and bots with artificial intelligence will lead to an increasing outpace of human risk assessment capabilities by machines.

It is often stated that we live in a digital word, after a digital revolution. However, it is more likely that we live at the beginning of a structural change because of this digitalization. Imagine a world with data about every economic transaction, about every personal interest, about every decision, available to analysis about the future. This would have a tremendous impact on risk modeling. It is not unrealistic to expect the availability of at least some of these data sets in the future (Mayr-Schönberger and Cukier 2013).

Industry 4.0, IoT, physical internet, augmented reality, and artificial intelligence are most likely only the first symptoms for this structural change. It is very likely that there are a large number of innovations upcoming, which are up to now either known by a very small community or even completely unknown.

The strategic knowledge development framework for Horizon Scanning Center was developed to keep pace with the exponential increase of innovation speed in the last years. The main reason for this increasing rate of innovation is that the knowledge management gets better and better. At the same time, multidisciplinary teams with increasing specialized experts work on large and highly relevant topics. A remarkable number of expected future innovations will create very large data sets, which can be used to improve the quality of future expectation. Thus, the better the data sets (in particular for simulations), the better the innovation management for new innovations.

References

Amanatidou, E., Butter, M., Carabias, V., Konnola, T., Leis, M., Saritas, O., Schaper-Rinkel, P., & van Rij, V. (2012). On concepts and methods in horizon scanning: Lessons from initiating policy dialogues on emerging issues. *Science and Public Policy, 39*, 208–221.

Dinter, B., & Winter, R. (2008). *Integrierte Informationslogistik*, *Business engineering*. Berlin/Heidelberg: Springer.

Dolinska, M. (2015). Knowledge based development of innovative companies within the framework of innovation networks. Innovation-management policy. *Practice, 17*, 323–340.

EFP. (2016). European Foresight Platform (EFP). http://www.foresight-platform.eu/. 11 Jun 2016.

Forst, N. (2014). Ein Vorgehensmodell zur Identifikation datenschutzrechtlich relevanter Informationsflüsse bei der Verwendung von Sozialen Medien im österreichischen Krisen- und Katastrophenschutz, Master Thesis, University of Vienna.

Garnett, K., Lickorish, F. A., Rocks, S. A., Prpich, G., Rathe, A. A., & Pollard, S. J. T. (2016). Integrating horizon scanning and strategic risk prioritisation using a weight of evidence framework to inform policy decisions. *Science of the Total Environment, 560*, 82–91.

Ghobadi, S. (2015). What drives knowledge sharing in software development teams: A literature review and classification framework. *Information Management, 52*, 82–97.

Göllner, J., Klerx, J. (2013). Second Design by Göllner, Klerx 07/2013 published in: Klerx, J., Göllner, J., Mak, K., Horizon Scanning for emerging risks in supply chain systems, in: Wilby, Blachfellner, Hofkirchner (Eds.), *Book of Abstracts*, *EMCSR-European Meetings on Cybernetics and Systems Research* (pp. 601–607). Wien.

Göllner, J., Mak, K., Woitsch, R.. Inteellectual capital management using knowledge scorecards: The Austrian National Defence Academy Showcase, 21st DEXA conference, understanding the human genome: A conceptual modeling-based approach, Bilbao, Spain, University of Deusto, 30 august–3 September 2010.

Göllner, J., Klerx, J., Mak, K., Meurers, C. (2015) „Wissensmanagement im ÖBH – Foresight in der strategischen Langfristplanung“ in „Schriftenreihe der Landesverteidigungsakademie“ 5/15, ISBN: 978-3-902944-57-3; in the style of FP7 proposal SecScan – Horizon scanning and foresight for security research (FP7-SEC-2013-1), Abb.1, S.8, 22 Nov 2012.

IBM. (2016). Big data analytics. http://www.ibmbigdatahub.com/infographic/four-vs-big-data

Klerx (2012). Presentation of policy implications, presentation, stakeholder workshop, ETTIS, FP7.

Klerx, J. (2015). Masterstudiengang Public Management: Lehrveranstaltung Umweltszenarien 3. Einheit: Foresight in der strategischen Langfristplanung 24.1.2015, Verwaltungsakademie des Bundes, Schloss Laudon, Mauerbachstraße 43–45, 1140 Wien-Penzing.

Koivisto, R., Wessberg, N., Eerola, A., Ahlqvist, T., Kivisaari, S., Myllyoja, J., & Halonen, M. (2009). Integrating future-oriented technology analysis and risk assessment methodologies. *Technological Forecasting and Social Change, 76*, 1163–1176.

Konnola, T., Salo, A., Cagnin, C., Carabias, V., & Vilkkumaa, E. (2012). Facing the future: Scanning, synthesizing and sensemaking in horizon scanning. *Science and Public Policy, 39*, 222–231.

Kreibich, R. (2009). Die Zukunft der Zukunftsforschung, Ossip K. Flechtheim – 100 Jahre, Arbeits Bericht Nr. 32/2009, Institut für Zukunftsstudien und Technologiebewertung (IZT), Berlin, 2009.

Mayr-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work and think* (p. 2013). London: Hodder and Stoughton Ltd..

McNurlin, B., & Sprague, R. (2002). Information systems management, 5th edition, prentice hall, Pearson education 2002. In *ISBN 0–13–034073-1*.

Meurers, C., Göllner, J., Quirchmayr, G., & Vogl, A. (2015). Wissensmanagement im ÖBH – Einführung in die Informationslogistik als Grundlage zur Wissens- und Organisationsentwicklung, Schriftenreihe der Landesverteidigungsakademie 20/15 (J. Göllner, C. Meurers, G. Quirchmayr, eds.), Vienna.

Mokrech, M., Nicholls, R. J., & Dawson, R. J. (2012). Scenarios of future built environment for coastal risk assessment of climate change using a GIS-based multicriteria analysis. *Environment and Planning B-Planning & Design, 39*, 120–136.

Palomino, M. A., T. Taylor, R. Owen & IEEE. (2012). Towards the development of an automated, web-based, horizon scanning system. 2012 Federated Conference on Computer Science and Information Systems (Fedcsis), pp. 1009–1016.

Palomino, M. A., Taylor, T., McBride, G., Mortimer, H., Owen, R., & Depledge, M. (2013a). Optimising web-based information retrieval methods for horizon scanning using relevance

feedback. In *Federated conference on computer science and information systems (FedCSIS)* (pp. 1139–1146). Krakow, POLAND: Ieee.

Palomino, M. A., Taylor, T., McBride, G., & Owen R. (2013b) Instability in search engine results lessons learnt in the context of horizon scanning applications. 2013 24th International Workshop on Database and Expert Systems Applications (Dexa 2013), pp. 53–57.

Pavlic, M., Han, Z. D., & Jakupovic, A. (2015). Question answering with a conceptual framework for knowledge-based system development "node of knowledge". *Expert Systems with Applications, 42*, 5264–5286.

Polemi, N., & Kotzanikolaou, P. (2015). Medusa: A supply chain risk assessment methodology. Cyber security and privacy. *Csp Innovation Forum, 2015*(530), 79–90.

Powell, J. H., Mustafee, N., Chen, A. S., & Hammond, M. (2016). System-focused risk identification and assessment for disaster preparedness: Dynamic threat analysis. *European Journal of Operational Research, 254*, 550–564.

Salzano, K. A., Maurer, C. A., Wyvratt, J. M., Stewart, T., Peck, J., Rygiel, B., & Petree, T. (2016). A knowledge management framework and approach for clinical development. *Therapeutic Innovation & Regulatory Science, 50*, 536–545.

Shi, Y. Q. & Y. L. Zhu (2013) A framework for development the open systems interconnection of integrated intelligent knowledge for management of networks. Information Technology Applications in Industry Ii, Pts 1–4, 411–414, 795–798.

Sutherland, W. J., Allison, H., Aveling, R., Bainbridge, I. P., Bennun, L., Bullock, D. J., Clements, A., Crick, H. Q. P., Gibbons, D. W., Smith, S., Rands, M. R. W., Rose, P., Scharlemann, J. P. W., & Warren, M. S. (2012). Enhancing the value of horizon scanning through collaborative review. *Oryx, 46*, 368–374.

Trawinska-Konador, K., Chlon-Dominczak, A., & Sienkiewicz, L. (2015). Development of the sectoral qualification framework as an example of a knowledge management approach. In *Proceedings of the 11th European conference on management leadership and governance* (pp. 496–503). MilitaryAcademy, Lisbon, PORTUGAL: Acad Conferences Ltd..

Uusitalo, T., Koivisto, R., & Schmitz, W. (2009). Proactive risk assessment of critical infrastructures. Safety, reliability and risk analysis: Theory. *Methods and Applications, 1-4*, 2511–2517.

Entrepreneurial Ecosystem: How to Improve Your Local Ecosystem with Political Initiatives

12

Florian Alexander Boesenkopf

Contents

Abstract

Currently, the terms entrepreneurial ecosystem and startup are of major importance for legislators, governments, and whole geographic areas. Nowadays, young, sustainable, and innovative startups can influence specific regions in respect to employment rates and HDI and GDP growth. However, an entrepreneurial ecosystem consists of different stakeholders and complex mutual rela-

F. A. Boesenkopf (✉)
influence.vision, iwondo and NoviSmart, Technology Scout for Bosch in Palo Alto, Vienna, Austria
e-mail: florian@novismart.com

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_38

tions. A fundamental issue for policy makers is how to promote the creation of those young successful companies and how to create a potent entrepreneurial ecosystem while persisting social equality. This analysis evaluates the stakeholders of an entrepreneurial ecosystem as well as the underlying startup phenomenon and derives a framework on three key social and political factors that can improve a startup network.

Keywords
Startup ecosystem · Entrepreneurial ecosystem · Disruptive technology · Startup · Innovation

Introduction

Since the financial crisis in 2008, the terms startup and disruptive technology are widely used as the savior of economic recession. Startups are on center stage to change the current financial outlook, and some of them even outperformed the highest expectations.

Major successes such as Facebook, Google, Uber, AirBnB, LinkedIn, and Apple are all headquartered within a 50 mile radius in Silicon Valley (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012; Saxenian 1996; Chen 2016). Young companies and their new technologies are able to significantly influence specific regions with respect to employment rates and human development index (HDI) and gross domestic product (GDP) growth. In other words, their ecosystems demonstrably advanced certain regions and cities like Silicon Valley, Berlin, or Tel Aviv (Compass.co & Crunchbase 2016). One of the main success factors of the startup phenomenon is a new approach on how to collaborate in a creative and open-minded network industry while levering the overall output through passion and ambition of each contributor and stakeholder (Florida, The Rise of the Creative Class 2012).

If the rise of startups and the so-called creative class that thinks outside the box are evidently so important, legislators have to drastically reassess the current political situation regarding innovation and entrepreneurs (Florida, The Rise of the Creative Class 2012). To be more precise, lawmakers should reconsider the existing free-enterprise system and adapt it to the current needs of technology-driven companies. Nowadays, whole industries can transform significantly within a few years. Governments must react accordingly as well as quickly to prevent severe negative effects on local industries.

However, to change a startup ecosystem, it is essential to be aware of the various stakeholders who contribute on the microeconomic level. The ecosystem does not only consist of startups but also of universities, private and corporate investors, media, and the respective government. All stakeholders must be addressed equally to make an entrepreneurial ecosystem successful (Compass.co & Crunchbase 2016; Roland Berger & Pioneers 2016; Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012).

In today's technology-driven world, several characteristics have transformed from the old economy. Formerly, a classic standard business produced and sold assets. Correspondingly, a substantial number of employees were required to produce these assets. Nowadays, major enterprises and startups, especially those that show the greatest growth in recent years, specialized on the facilitation of physical assets rather than on the production. Uber (Uber is a platform that allows people to share peer-to-peer private taxi services (Uber Technologies Inc. 2016)) currently valued over 65 billion USD, and AirBnB (AirBnB is a platform that allows people to rent (short stays) out peer to peer their apartment/house (Airbnb, Inc. 2016)) valued over 20 billion USD do not own any tangible assets. Both startups are merely a platform that helps users find each other to facilitate resources that are currently not used.

As an example, Uber has a higher enterprise value than car manufacturers like FORD, GM, or Honda. Figure 1 illustrates the comparison between car manufacturers' and Uber's valuation (Chen 2016; Winkler and MacMillan 2016). Startups such as AirBnB and Uber benefit from the network effects that occur when assets are facilitated peer to peer. A great part of their high valuation comes from further possibilities of leveraging their current network and user base. Uber, for instance, had weddings on demand and is lending cats to cuddle for Uber users from Uber users (Chen 2016).

Startups ultimately do not need a lot of man power but therefore in exchange highly specialized and outstandingly educated talents. On the social level, the education singularity retrieves certain risks on equality in the society. This is a clear downside of a technology-driven entrepreneurial ecosystem. Governments should closely monitor this phenomenon to obtain social equality. In this context, administrations need to promote cyber development through entrepreneurial ecosystems. Knowledge and education are a core value for startup success as well as the development of a knowledge economy, knowledge society, and knowledge democracy. Globalization is a clear growth opportunity in an interconnected world.

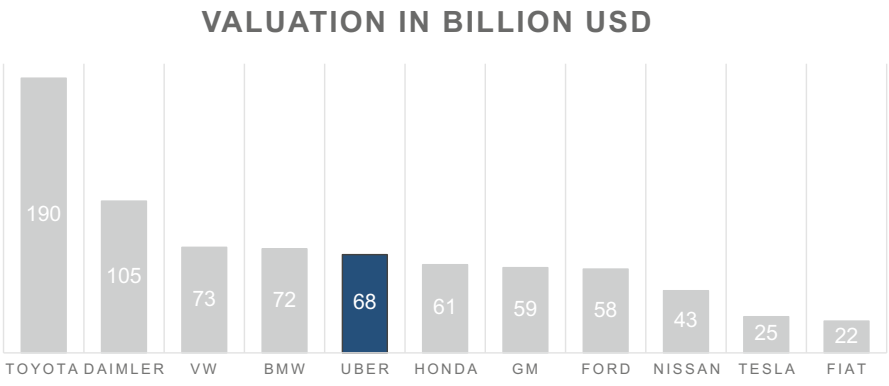


Fig. 1 Valuation of car manufacturers/facilitators in accordance with Chen (2016)

Consequently, governments should open the job market for international knowledge migration of tech talent.

However, the term network is not only indispensable for new technologies but for the entrepreneurial startup ecosystem itself. Regions such as Baden-Württemberg in Germany or Silicon Valley in the USA have established dynamics of regional network-based industrial systems. This system consists of a horizontal network of firms that are mainly specialized in certain fields. In contrast to most business relations in network-based ecosystems, startups collaborate closely but without exclusive arrangements. This phenomenon is similarly a core characteristic of open source technology (Saxenian 1996; Shapiro and Varian 1999; Florida, The Rise of the Creative Class 2012).

The explicit research question for this analysis is how legislators and governments can improve the formation of startups and entrepreneurial ecosystems through political initiatives. To deviate implications and answer the research question, the analysis evaluates the entrepreneurial ecosystem and explains the main reason for the startup phenomenon. The analysis will discuss the change from an Industry to an Information Revolution explaining network effects, the facilitation industries, and the rise of the creative class and social equality.

Subsequently, a framework is developed on how to improve a local entrepreneurial ecosystem. The scheme provides stakeholders in the startup network, especially governments, with actionable activities and a reference book.

Startup Ecosystem

The startup ecosystem is a complex system with mutual relations between all stakeholders. Correspondingly, it is important to understand and analyze each individual participant in the ecosystem to realize the overall impact of each contributor. Universities, governments, corporations, and media are the providers or platforms of the network. Entrepreneurs are the clear leaders that should direct the long-term success of the ecosystem. Both leaders and providers in the startup ecosystem are of equal importance. The collaboration between all stakeholders is essential for a thriving entrepreneurial spirit but needs control as well as social and political structure. In the following, the various stakeholders are further analyzed (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012) (Fig. 2).

Entrepreneurs

Entrepreneurs have the leading role in the startup ecosystem. They are the driving factor and set the path for long-term success. Ultimately, they must engage with all stakeholders to improve the conditions in the ecosystem. Furthermore, entrepreneurs should make room for novel ideas, innovations, and a new generation entering the market (Florida, The Rise of the Creative Class 2012).

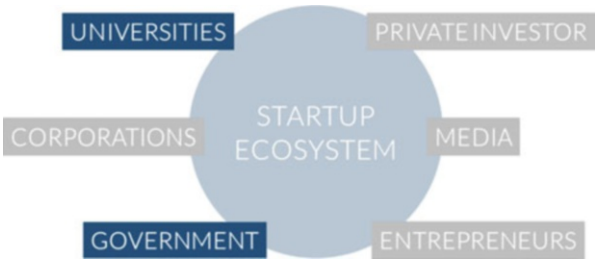


Fig. 2 Startup ecosystem (author's illustration)

At this stage, it is also essential to define the term startup. Although there seems to be no clear definition, the term startup is used frequently over the last several years. First of all, it is essential to state that there is a distinct difference to a small business. Startups aim for a new window of technology and want to disrupt a market with a completely new product, process, or service. Correspondingly, the failure rate of startups is considerably higher. While two thirds of small businesses survive, only 10% of startups do. Ries (2010), for instance, defines a startup as an organization that faces extreme uncertainty (Ries 2010).

Moreover, the business model of a startup is scalable, and expansion as well as internalization is usually a key strategy. Graham (2012), for example, states that enormous growth is the only criteria that must be fulfilled in order to be considered as a startup. Under this definition, Facebook founded in 2004 is still a startup. Furthermore, entrepreneurs approach innovation, technology, and business models in a unique manner and are constantly looking for a new and better solution. To call your business a startup, it should be typically founded within the last 3–5 years. In terms of industry, there is no limit for startups. Although most popular and successful startups of the last 20 years have its origin in the information technology (IT) industry, the term is not restricted to this field of business (Robehmed 2013; Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012; Graham 2012).

Another understanding of the term is the inferred mind-set. Startups operate in a unique and collaborative network of companies with completely new business structures. These companies operate as networks rather than under hierarchies. Entrepreneurs emphasize on impacting actions instead of control. At the same time, entrepreneurs are self-aware of their weaknesses and therefore share them openly with the community to straighten these weaknesses. The general principle is "give before you get" (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012).

Entrepreneurs are exposed to enormous financial pressure. At the beginning, there is not a lot of room for failure. To be successful, a startup should be aware of all stakeholders. Investors are important to raise money and to stay financially independent, and universities are essential to acquire talent and get research access. Governments give startups financial support, and they are vital concerning tax and regulatory compliance. In turn, media leverages the business opportunities with the

possibility of accessing a broader audience. The mutual relation becomes specifically visible over the leadership position of the entrepreneur.

Investors

Money is inevitable to start a company because of several reasons, but it is not the main success factor in a startup. Consequently, investors are certainly not the most important driver in an entrepreneurial ecosystem. It is a common misconception of entrepreneurs that there is not sufficient capital in the ecosystem to start a company. For investors on the other hand, it is important to understand that success only exists in the long term. Venture capitalists must realize that a lot of effort is required to improve the perception that there is sufficient capital available in the ecosystem (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012; TED Talks 2015). Generally, there are three types of financiers: private, institutional, and corporate investors.

First, why do startups need investors? The early days of a startup are usually financed by the entrepreneur or the so-called 3Fs (family, friends, and fools). Taking out a loan is not an option at this point because banks are committed to legal solvency policies. So startups face certain challenges to overcome these financial hurdles.

In terms of the life cycle of a startup, the investment or venture capital process can be separated into three stages. In each of these stages, startups have different financing requirements and correspondingly need diverse investors to grow effectively. The categories are the seed, the startup, and the expansion investment phase. Figure 3 illustrates the process over the startup life cycle including the typical capital requirements and investors (Jeng and Wells 2000).

In the first two phases, the businesses are still in an early stage. In the seed stage, entrepreneurs are typically in the research and development process for their service or product. Companies merely have an idea but not a proven business model. In this phase startups need an investor to finance a prototype to get access to research labs or workspaces. At this stage an accelerator or incubator can support the development of an idea. The next phase is the startup stage which refers to entrepreneurs that established a product or service but have not yet successfully commercialized it. In this period, startups might have first costumers but are far away from reaching the economic breakeven. In general, entrepreneurs at this stage mainly require financial support to successfully market their services or products but similarly need the urge for business know-how (Jeng and Wells 2000).

In the expansion stage, startups typically have a base of a paying clientele in a certain geographic area. At times, they are even profitable. However, the internal financial cash flows and outside financing possibilities are not sufficient to expand internationally. In order to compete against international and mature competitors, startups frequently aim to expand globally. Hence, entrepreneurs require larger investment rounds compared to the first two stages as well as international experience to scale the business at a global level (Jeng and Wells 2000).

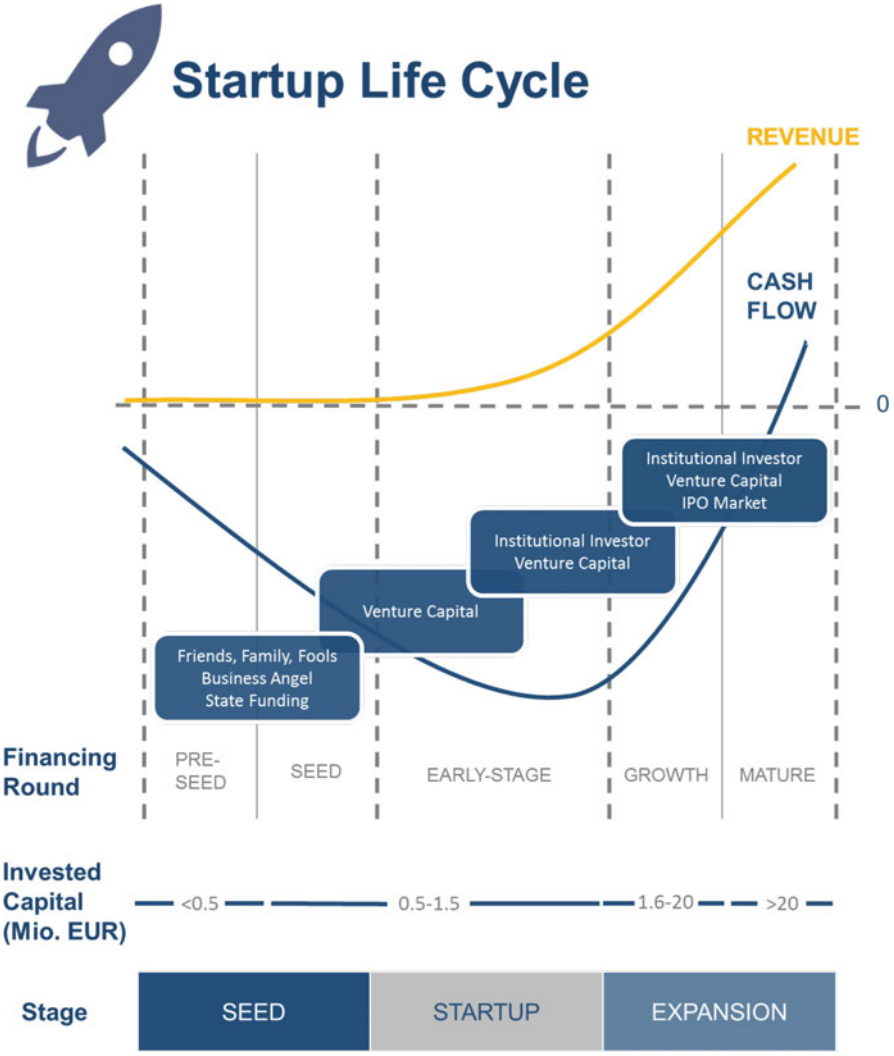


Fig. 3 Startup life cycle in accordance with Roland Berger & Pioneers (2016)

Private Investors

Private investors are mainly business angels who are often entrepreneurs themselves. Besides business angels, there are two stakeholders which can be classified as private investors, namely, family, friends, and fools as well as crowdfunding platforms (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012; Compass.co & Crunchbase 2016; Roland Berger & Pioneers 2016). Crowdfunding networks such as Indiegogo or Kickstarter allow startups to present an idea or a rudimentary prototype. The "crowd," namely, everyone who is visiting the public website, can then donate money or invest in the project (Barnett 2014).

Smaller investment rounds in the seed stage are characteristically for private investors. However, especially business angels further support entrepreneurs as mentors or business advisors. At this point of the startup life cycle, it is extremely difficult to foresee the success of a company. Accordingly, the private investors' risk and potential reward is comparably high.

Corporate Investors/Partners

Corporations work together with startups in different forms. The main types of collaborations are acquisitions, corporate venture capital (CVC) investments, or partnerships. Within this classification, corporate partners of startups are categorized as investors because they typically pay for the development of a product or a service. In other words, this is a kind of non-equity transforming investment (Berk and DeMarzo 2014).

The major difference between an acquisition and a venture capital investment is the percentage of ownership and control. In an acquisition, typically 100% of the equity is transferred to the acquirer. Consequently, the entire control is devolved to the corporation purchasing the startup (Haspeslagh and Jemison 1993; Faccio and Masulis 2005; Kaplan and Stromberg 2003). In contrast in a venture capital deal usually only a minor equity stake is bought (Gompers and Lerner, The determinants of corporate venture capital success: Organizational structure, incentives, and complementarities 2000). The startup still is in control of all major decisions. Through venture capital investments, corporations have a higher flexibility and option to either engage further with the startup or to liquidate or rather sell the equity stake (Kaplan and Stromberg 2003). At the same time, entrepreneurs have a comparably high degree of freedom for the development of their company (Berk and DeMarzo 2014).

Another upcoming trend concerning investments in entrepreneurs is acquihire. It is a hybrid form of acquiring a startup and hiring the key personnel of it. The term emphasizes the importance of highly experienced founders and their creative ideas. This method can be outlined as hiring with a substantial signing bonus. Frequently, the actual startup is liquidated after the transaction, and the key people are taking over other roles in the acquirer's business (Feld, FeldThoughts 2015).

In comparison with institutional investors, corporations typically do not have a solitary financial objective. The integration, the investment cycle, and the collaboration are typically more extensive compared to primary financial venture capital investments. Consequently, for corporations it is essential to have a strategic purpose in their partnership with entrepreneurs. To successfully operate a venture capital arm, a corporation needs to make target investments in startups that can be leveraged by internal knowledge as well as core fundamental research and development (R&D). Nowadays, corporations see venture capital or partnerships with startups as a third pillar of innovation next to acquisitions and R&D (Roberts 2006).

Institutional Investors

Institutional investors influence the business development as well as the decision-making process of a startup in a powerful manner. Consequently, these venture

capital funds (private equity) differ significantly from public equity funds that act comparably passive (Jeng and Wells 2000).

Institutional venture capital funds are usually established by an investment bank. VCs have pure financial objectives, and correspondingly the main goal is to increase shareholder value. Other than corporate investors, institutional investors generally do not have a strategic goal. Quick exits are a genuine venture capital principle (Lerner 2013). In addition, VCs enter numerous markets and invest in a diverse portfolio of entrepreneurs in order to diversify risk.

Venture capital funds typically invest in the expansion phase of a startup with higher investment sums. In 2011 US venture capital funds invested in average 7.7 million USD per startup transaction (Berk and DeMarzo 2014).

Government

Governments have two core responsibilities in an entrepreneurial ecosystem. However, the competences are to some extent contrary. On one hand, governments are a quasi-investor and offer various financial supporting programs to startups. On the other hand, legislators slow down the innovation network because of regulations and tax laws. Nevertheless, both activities are of equal importance to keep a startup ecosystem in balance.

A major friction and pain point between startups and administrations is the different time constraint. To develop a disruptive technology, young companies have to be extremely agile and lean in their cost structure. An early adaptation to market variations is of great relevance. To do so, entrepreneurs need a maximum degree of freedom to ensure to be financially solvent and thrive on the existing innovation and business opportunities (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012). Although in various countries legislators work on improved conditions for startups and researchers, the government leaders typically fail to support the ecosystems sustainably in the long term. Policy leaders have a different objective as they usually take office for a limited period. In summary, governments have completely different life cycles, objectives, and mechanisms that are somehow contrary to startups. Correspondingly, the most frequent mistake is that policy makers do not really know the problems and needs of startups (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012).

As a hybrid investor, governments play a major role for entrepreneurs, especially in the seed stage. Venture capital funds and funding agencies backed by national budgets often take substantial risks and therefore provide a fundamental contribution to young founders and their ideas. Additionally, governments often collaborate with universities and research facilities to promote research and development. The investment in R&D as well as education is a good breeding ground for the next generation of entrepreneurs (Compass.co & Crunchbase 2016; Roland Berger & Pioneers 2016).

Universities

Educational, cultural, and administrative facilities play an important role in an entrepreneurial ecosystem. There are certain success stories such as Silicon Valley which is strongly connected to Stanford, Route 128 closely collaborating with Harvard and MIT, or London leveraging LSE and Cambridge (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012). However, there are also upcoming areas such as Berlin, Copenhagen, or Vienna leveraging on the heritage of their educational systems (European Startup Initiative (esi) 2016; Compass.co & Crunchbase 2016).

However, universities should not be considered as leaders of the startup ecosystem but rather as a platform of talent, infrastructure, motivation, and innovative ideas. In other words, educational facilities are providers for the entrepreneurial network. To sum it up, universities have two properties which are a contribution to the community: people and facilities.

The property people consist of professors and students. Each year new graduate students further enhance the community. They either actively participate in a startup or passively improve the mind-set for collaborations with young companies. On the other hand, professors are able to mentor startups and help young entrepreneurs in their research to protect their intellectual property (IP). Habitually students start companies based on the basic research of their faculty. Professors are often entrepreneurs themselves or actively support startups as advisors.

Facilities are built of various parts such as laboratories for research, technology centers, incubators, libraries, and lectures focusing on entrepreneurship (Business Model Creation, Pitching, Venture Financing, etc.) (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012). For instance, the Technical University of Vienna started the i2c entrepreneur support program in form of an innovation incubation center. The center provides labs, enables mentoring, and gives young founders of startups access to capital (Roland Berger & Pioneers 2016).

Furthermore, universities often have very inefficient IP or technology transfer offices. They either take too much time to file a patent or have enormous expectations about IP licensing agreements. In either case, it can be fatal for a startup or a spin-off project and sometimes even kills the idea before it even started (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012).

Media

Media has a unique role within the startup ecosystem. They are neither a leader nor a provider but rather an accelerator of the network. Newspapers, blogs, magazines, social media, and TV stations are the speaking tube of the entrepreneurial network and amplify the magnitude of the startup movement in the public perception. Media can change the perception as well as the mind-set, and it motivates young researchers and students to found their own companies. Furthermore, it opens the window on the

acceptance of entrepreneurship and establishes courage as well as role models to young founders.

In addition, media is the platform for the collaboration of startups and investors such as crowdfunding programs. Within a few clicks, the whole world can invest in an idea. Sharing of knowledge has never been easier. Especially the Internet allows founders to enter industries with comparably higher entry barriers through a large amount of information being available through it.

Media companies sometimes even serve as a quasi-investor. Especially newspapers and TV stations offer a "media for equity" program. In return for equity, startups get broadcasting time or advertising space. In countries, such as Austria, Germany, or the USA, there are even TV shows specialized on startups. In these programs, young entrepreneurs can pitch in front of a jury of investors (Roland Berger & Pioneers 2016).

Industry to Information Revolution

The Industrial Revolution is long over, but the spirit of a new transformation, namely, an Information Revolution, is present like never. The transformation is similarly referred to as the Creative Revolution. At times where data and software applications are more valuable than tangible assets, there is clearly a groundbreaking change happening. The main actors in an ecosystem have been analyzed in the previous section. Without a doubt, startups are the most crucial factor in this new evolvement (Florida, The Rise of the Creative Class 2012).

However, the question how disruptive technologies and developments demonstrate this monumental transition is still unanswered. So, what are the drivers in the Information Revolution? Similarly to the Industrial Revolution, how does it change the job requirements as well as the social structures? In this section the driving effect of the entrepreneurship phenomenon will be explained.

Network Effects

Technological Network Effects

One of the leading technologies which is responsible for the Information Revolution is network effects. Starting from telecommunications to the Internet to social media, network effects have been the underlying constant for success in innovation in recent history. To understand the startup ecosystem, it is essential to analyze this phenomenon and its mechanisms.

The researchers Shapiro and Varian (1999) derived the value of a network with the following equation which is expressing the exponential relation between users and a network (the methodology is derived from the Metcalfe's law. Bob Metcalfe was the originator of the Ethernet. The computed value through the function is merely an estimation and should not be taken as an exact figure) (Shapiro and Varian 1999):

$$\text{Value of a network} = \text{user} * (\text{user} - 1) = \text{user}^2 - \text{user}^3$$

Networks have a virtual structure that involves a sponsor and a certain number of users typically starting with at least two. The community is created by the sponsor who is accountable for its conditions. The sponsor does price, user registration, and the development of the platform. Shapiro and Varian (1999) proved that if a network passes a certain number of users, the value of the network relates positively to user fidelity. They refer to this phenomenon as the demand-side economics of scale. In other words, with an increasing number of participants in a virtual system, the incentive to enter and actively take part in a network increases significantly.

Once this critical mass of users is reached, the existing participants in the virtual community subliminally influence new users to join the network and further enhance the value of the network. This effect is called network externality (Shapiro and Varian 1999; Gompers and Lerner, The Venture Capital Cycle 2002). Messenger applications are a recent example for a successful virtual community. The more participants download the application, the higher is the probability and the incentive for a new user to purchase the messenger service. Once a startup is in a leadership situation, the virtual community can be used for cross-selling opportunities for other products in the pipeline.

The ideal example of a messenger service startup is WhatsApp. In 2009, Jan Koum and Brian Acton founded WhatsApp as the first messenger application to allow the sharing of messages, pictures, and videos over the Internet. Correspondingly, no extra charges from telecommunication providers occurred, and it was easily possible to share information internationally (The Economist 2014; Kuchler and Bradshaw 2014). The company was acquired in 2014 by Facebook for 19 billion USD. At this time, the company had only 32 employees. Each staff member was facilitating 14 million users (The Economist 2014; Anders (a) 2014; Kuchler and Bradshaw 2014).

With their unique strategy, the startup quickly became the fastest user expanding network in the world. The growth in comparison with industry competitors is illustrated in Fig. 4. To achieve this huge success, WhatsApp pursued three key policies. First, there were no advertisements in the application, it was free of charge, and finally they had a first mover advantage by expanding quickly to different operating system platforms (i.e., iOS, Android, Windows). Following this strategy and aligning to the market needs of an international option to communicate effectively, WhatsApp establishes the fastest rising network in history. Their achievement can be explained through the high retention numbers. Seventy-two percent of daily active users send 100 million videos, 200 million voice mails, and 500 million messages. In other words, WhatsApp processes more messages than all mobile providers worldwide combined (Anders (a) 2014; The Economist 2014; Kuchler and Bradshaw 2014).

However, at the beginning the friction of a network to persuade new users is enormous. WhatsApp is an encouraging example, but there are also examples which have been less successful. To take the effect of competition into account, it is

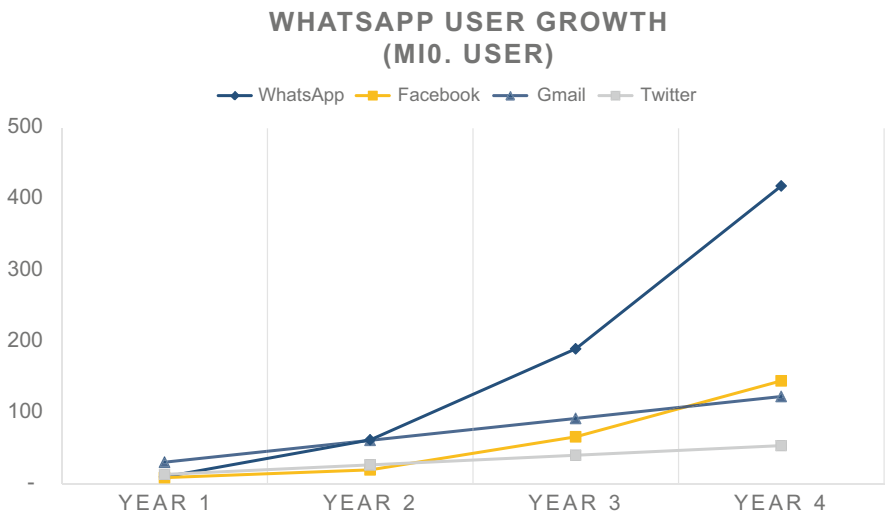


Fig. 4 WhatsApp user growth in accordance with Forbes Anders (a) (2014)

essential to include the cost of substitutes in the context of network effects. Nevertheless, as the number of users increases, the influence of substitutes decreases accordingly. In general, the substitution fear in the technology era was higher before the Internet. When the telephone was invented, the cost of switching to another virtual community was clearly higher in comparison with messenger applications (Shapiro and Varian 1999). In modern networks, especially concerning smartphone applications, the costs of substitution are nearly equal to zero. The low entry barriers and substitution risks allow new virtual communities to grow at an extensive rate which is one of the essential comparative advantages in today's networks (Davenport et al. 2010).

Even former network giants have a hard time competing against startups in the virtual industry. Yahoo, for example, was valued in 2000 at 125 billion USD. In 2016, Yahoo sold itself at financial distress to Verizon for roughly 4 billion USD. Once believed to have won the battle of search engines, they ultimately could not compete against the overwhelming power of Google and its rapidly growing network. Google simply leveraged the rising system of connections to overtake the search engine thrown. Notwithstanding, in market with nearly equal to zero substitution costs and rapidly expanding startups in the network industry, Google is also not certain to succeed in the long term (Choi 2016).

Network-Based Industrial System

The network-based industrial system which is similar to the technological network influences the entrepreneurial ecosystem fundamentally. Although startup communities are typically clustered in one specific area, the network-based industrial system

enhances globalization and internationalization through the strongly linked collaborations with industry peer groups.

The system consists of horizontally structured firms that are highly dedicated to one specific field of expertise but nevertheless cooperate with the network participants. However, the partnerships are not exclusive. They still allow companies to quickly engage with various entrepreneurs. Other than independent corporations that generally undertake most business activities internally, participants in the industrial community seek out to partners for expertise in fields they are not entirely familiar with (Saxenian 1996).

A well-known historical example for a network-based industrial network is the Japanese keiretsu. This system is especially common in the automotive and electronics industry, having several key suppliers collaborating on inclusive engagements. In a keiretsu, partners even hold syndetic equity shares to ensure trust and common objectives (Berglöf and Perotti 1994).

Similar to keiretsus, the loose relationships in an entrepreneurial community allow startups to quickly engage with partners and subsequently enter new markets. Additionally, this is a form to share knowledge and collaborate on joint technology projects such as open source software. Leveraging this singularity and the effects of knowledge spillovers, startups can exploit a pool of talent and technology that were inaccessible for young business owners in the past (Saxenian 1996).

From Production to Facilitation

For a long period, the production of assets has been the primary business model in Western economies. However, in today's industrialism a lot of key markets are saturated. Corporations in sectors, such as the automotive or real estate industry, face enormous competition as well as sales difficulties. Growth levels are declining and revenues are stagnating (Shapiro and Varian 1999).

In order to adapt to the market needs, the most successful entrepreneurs in the information era have adopted their business models to simply facilitate assets instead of producing and distributing them. The timing of this business model invention was an essential key for prosperity as the singularity of sharing arose in the middle of the financial crisis in 2008. Platform facilitating businesses have lower overhead costs and thus are poised for rapid growth. In recent history networks, such as Uber and AirBnB have accomplished massive profits with the facilitation of assets. As sponsors the startups operate a platform to connect people. Both entrepreneurial-driven companies grew quickly enough to outperform competition and kept substitution prices low (Chen 2016; TED Talks 2015).

The nature of the information industry requires typically less employees to undertake a business but therefore highly specialized and well-educated experts. In other words, the workforce in this sector of facilitation assets is completely different to producing assets nonetheless significantly better paid due to comparably high growth rates (Florida, The Rise of the Creative Class 2012).

Rise of the Creative Class

In the Industrial Revolution, jobs were taken over by machines. Before the Industrial Revolution, hand production methods did the manufacturing of goods. With the invention of the steam engine, chemical manufacturing processes, and sophisticated factories, the productions have been automated. However, not only economically but also in terms of education, wealth, and equality this revolution brought changes to the social order (Ashton 1998). The Information Revolution is creating a similar phenomenon. Data and computer algorithms take over ordinary office jobs and change the job and social requirements as we know it from today.

Chatbots, for example, are set to change the way we communicate with service providers. Ninety percent of the time spent with smartphones is used to write messages, from e-mails to applications such as WhatsApp. Leveraging on this trend, Chatbots are artificial intelligence services that can automatically respond a request or inquiry. For instance, the clear majority of call center activities could be undertaken by Chatbots. The number of employees which is required would reduce significantly. There are startups which apply this technology for accounting, real estate brokerage, e-commerce, and news (Schlicht 2016; Mehr 2016). Open source communities are a similar example for an information change. Through publicly sharing source codes of a specific and typically free software, every member of the community can actively participate in an open alliance to improve, write, and change the software. In a joint effort, technical bugs, obstacles, and issues can be resolved quickly and easily (Opensource.org 2016). The media revolution in form of social media is another milestone in the creative revolution. There is simply more data available, and the content is less professional allowing individuals to rapidly share news and events on the spot throughout virtual communities (Kietzmann et al. 2010; Kaplan and Haenlein 2010).

Nevertheless, the Information Revolution similarly entails a social transformation. Creative is the most used word for a personal description on the professional network platform LinkedIn. Creativeness is a core attribute in today's economy since it is one characteristic of humans that cannot be replicated by an artificial computer algorithm. Nowadays, most people in the entrepreneurial scene work and live like artists or scientists focusing on the creation of new sustainable values. Essentially being creative indicates a lot more than arts, but it is a core quality within professional fields such as information technology, coding, management, marketing, and research and development. Furthermore, it is a social enlargement as the fundament of creativity is built upon diversity, openness, and sustainable progress, key characteristics of an entrepreneur. For instance, the social and urban scientist Richard Florida (2012) identified that an active gay community significantly affect the real estate prices in an area. Prices evidently tend to rise implying a certain tangible value in the presence of diversity. Furthermore, an active music scene has become an indicator for a potential innovation hub. There is a profound and significant correlation between artists living in a city and technologic development in terms of capital invested, patents, and human development. The enrichment of art positively

influences creativity even outside of the art scene. San Francisco, Berlin, and Vienna, for example, have not been a stranger to music or theater and are a home to numerous artists. The diverse and open backgrounds of these cities have positively influenced the entrepreneurial scene and build a fundament for startups to think creatively. Basically, entrepreneurs are artists in many ways focusing on business-related topics (Florida, The Rise of the Creative Class 2012).

The rise of the creative class is a phenomenon of a new generation of well-educated and well-cultivated people working in a creative ecosystem. Moreover, the demands of the creative class influence the job and living condition requirements. Cross-employment, flexible working hours, as well as a solid work-life balance are inherent parts of the creative class. This social movement has become a centerpiece of modern cohabitation and can further determine the success or failure of a company's innovation strategy. The creative class is an enabler of innovation and technologic progress. Fostering and integrating this phenomenon is an important factor to be successful as a startup and further as any participant in the entrepreneurial ecosystem (Florida, The Rise of the Creative Class 2012; Campbell 2013).

Social Equality

In the Information Revolution, the decision where to live has never been more intriguing and important in a person's life. Another characteristic of this movement is urbanization. A lion's share of the creative workforce lives in or near to cities which are known for their network-based industrial system (Florida, Who's Your City? 2008; Saxenian 1996).

However, as the number of creative jobs rises which are habitually higher paid and the number of middle class jobs declines, the income and education gap ascends. The difference is particularly visible in countries such as the USA where high-level education is nearly unaffordable for the average American citizen. This singularity is less developed in Europe or Asia. Consequently, startup hubs such as Silicon Valley could convert in an artificial bubble in terms of social equality. With incredible high costs for housing, it is nearly impossible for someone outside of the creative class to participate or even live in the entrepreneurial ecosystem of Silicon Valley (Florida, The Rise of the Creative Class 2012).

Similarly, although industry entry barriers are falling, new unbridgeable social entry barriers are arising. This phenomenon is specifically crucial as the decision of where to live shapes the outcome of a young person's destiny (Florida, Who's Your City? 2008). Unfortunately, finding home in the creative class is not only a question of hard work in combination with technical expertise but also of wealth and social belonging. Numerous successful entrepreneurs come from rich families having easy access to the entrepreneurial ecosystem what makes it easy for them (Levy 2016).

This is not merely a social issue but a long-term challenge for a whole startup ecosystem and geographic area. The fundament of the creative class, innovation, and entrepreneurship is inclusiveness, diversity, and a network of highly passionate

contributors. Nevertheless, in the long term, if a certain group is unable or even knowingly not allowed to participate, the characteristics of diversity and inclusiveness will soon disappear, limiting the possibility for new technologies to arise and rapid progress (Florida, The Rise of the Creative Class 2012).

How to Improve Your Local Entrepreneurial Ecosystem

From 1990 to 1999, the NASDAQ-100 (National Association of Securities Dealers Automated Quotations-100), the main technology stock exchange in the USA, accomplished a return of around 30% year over year. The S&P 500 (Standard & Poor's 500, an index that can serve as a proxy for the market) in the meantime rose by less than 15% annually. In 2000 the dot-com bubble burst and the NASDAQ dropped by more than 40% (Yahoo! Corp. 2015). The startup industry that was alleged to be indestructible collapsed within 1 year. In other words, the technology itself is not the main factor to save an economy in the long term, but all stakeholders in the entrepreneurial community combined can make a sustainable impact to a region. During the dot-com bubble, the industry had been overvalued, and entrepreneurs took advantage of the situation. Rather than leading with long-term focus in mind, startups choose short-term financial benefits disregarding the future of the industry.

To make an ecosystem thrive, it is inevitable for each stakeholder to be aware of its role and the tasks as well as issues from the other contributors. Entrepreneurs are clearly the leader of the ecosystem and correspondingly should have the possibility to pursue certain strategic targets. If entrepreneurs fail to lead the community with long-term vision, the absence of direction can disable the whole ecosystem as it was the case in the dot-com bubble. On the other hand, the providers of the entrepreneurial community should be aware that they cannot act or fill in for startups as leaders without causing serious damage to the community. The core innovational and entrepreneurial movement has to be initiated by startups.

Additionally, it is essential for an innovation ecosystem to differentiate from other communities in terms of certain industry capabilities. For example, Baden-Württemberg is famous for its automotive industry, Los Angeles for media, and Silicon Valley for digital products (Compass.co & Crunchbase 2016; Saxenian 1996).

Teach Interdisciplinary Entrepreneurship

The field of entrepreneurship is interdisciplinary and should be outlined with respect to various industries and academic topics. Universities and educational facilities should establish programs throughout all different fields to explain and teach how to start a company. If a university creates a competence center for entrepreneurship, it should be located outside of the business school and encourage students to

collaborate between diverse fields (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012; Roland Berger & Pioneers 2016). For instance, the University of Vienna and the Technical University of Vienna started a collaborative program called INiTS service for startups. Together with the funding agency of the city of Vienna, the two universities jointly help startups to find the right talent and evolve their ideas into companies. In the last years, they have supported 185 startups, filed 383 patents, created, and assisted their entrepreneurs to raise more than 300 million EUR in venture capital. This results in an average deal value of 1.6 million EUR.

With their joint program, they have been awarded as the third best in Europe and seventh best global university business incubator. The unique mixture of technology know-how from the Technical University and social science experience from the University of Vienna has brought founders from all over Europe, especially from Eastern Europe, to Vienna and enriched the local ecosystem in terms of diversity considerably (iNiTS Universitäres Gründerservice Wien GmbH 2016).

Furthermore, there is a synergistic effect of being a professor and an entrepreneur at the same time. This can be highly beneficial for a local ecosystem (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012). These synergies can further be influenced by the concept of cross-employment. If a professor is employed at two organizations, he/she can diversify as well as complement creative knowledge and create a more miscellaneous network. Correspondingly, the knowledge creation becomes, other than under the concept of Vannevar Bush (1945), nonlinear (Campbell 2013; Vannevar 1945). Within this open mindset, a hybrid catered professor can further encourage students to found their own companies and elaborate on their ideas.

Align Objectives

The stakeholders in the entrepreneurial ecosystem have dissimilar objectives and demands. In order to jointly improve a startup community, all contributors need to align their long-term goals.

Time

Governments, entrepreneurs, and corporations have different time motivations. Government officials are elected for a certain term, typically for 4 years. Although corporations operate under the going concern principle, the well-known principal agent problem ascends as managers are in fact in charge for a limited period (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012).

At the very beginning, young startups contrariwise have a clear short-term focus. If someone starts a company, it is not ensured that it will survive the first year. A lack of financial resources and upcoming competition are just two factors which can determine the success or failure of a startup. In particular, the information technology industry is moving rapidly, and adapting to the market needs is essential to survive (Compass.co & Crunchbase 2016).

Corporations that want to invest or partner with a startup need to be aware of this lack of time entrepreneurs are typically facing. Generally, corporations have a long reviewing process, and by the time an investment is signed off by the responsible managers, the startup often is either in financial drought or outperformed by competition (Roland Berger & Pioneers 2016).

Similarly, entrepreneurs spend a large part of their time, especially in European systems, to legally form the startup. If a startup wants to recruit foreign talent, it has to overcome severe hurdles. Legislators have to simplify regulations for the formation of innovative companies in particular in rapidly moving industries in order to sustain a competitive environment in the ecosystem. Furthermore, equity of the startup is often the only possible method to compensate the first employees. However, in most countries it is extremely difficult and complicated to transfer equity legally, especially to foreigners. As described a comparative advantage in network-driven fields is often generated through extensive and quick market penetration which can be destroyed through long and bureaucratic official channels. Furthermore, the friction to hire foreign talent needs to be addressed and even incentivized or at least supported by the government. A multinational workforce adds diversity to the ecosystem and consequently enriches the range of ideas and innovational power (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012; Compass.co & Crunchbase 2016).

Financial Incentives

As time, capital is a scarce resource for entrepreneurs. At the beginning of the startup life cycle, little investments can make a severe difference and are pivotal for the success of an entrepreneur. Furthermore, most of the money invested or generated in the company is immediately spend in the ecosystem. This situation has to be incorporated by government officials in order to keep costs for the formation of the corporation, legally required capital for limited liability as well as fees and taxes affordable. Furthermore, tax authorities could introduce tax concessions for investors that actively participate in the ecosystem by investing in venture capital (Compass.co & Crunchbase 2016). For corporations to support promising startups through the long review process, managers could make small investments in form of nonrecurring engineering engagements. Consequently, the entrepreneurs would have the chance to operate effectively and without losing the competitive edge on the technological expertise. The concept of the academic firm provides a framework for corporations to apply a knowledge-driven strategy that allows corporations to closely collaborate with universities and startups. In the academic firm, the key objective is not to primary increase shareholder value but to improve knowledge. As a by-product shareholder value rises instinctively, corporations should consider the framework of the academic firm when cooperating with young enterprises and academic institutions (Campbell and Carayannis 2016).

Entrepreneurs occasionally have a misperception that there is not enough capital in a certain ecosystem. Although, this can be the case in upcoming areas, typically this is not the reason for a good idea to fail. Investors and their money usually go where opportunities are. In other words, entrepreneurs are always able to seek for

money outside of the local ecosystem. Companies should understand this early-stage mechanism to improve long-term local capital availability (Feld, Startup Communities – Building an Entrepreneurial Ecosystem in your City 2012).

Intellectual property (e.g., patents, trademarks, etc.) is a substantial element of the value of an early-stage enterprise and one of the critical determinants for the success of entrepreneurs (Sievers et al. 2012; Block et al. 2013). Copyrights, trademarks, and patents are the legal fundament to protect an innovation. Legislators as well as universities must protect the ecosystem's IPs and support entrepreneurs to file patents and protect their technology. Eventually, the knowledge can be further leveraged within the industrial-based local network (Shapiro and Varian 1999).

3T Framework

The 3T framework consists of three parameters that individually and jointly influence the entrepreneurial ecosystem. It can be applied in two forms, either to evaluate the complete startup community or each stakeholder on its own. However, the indicators for the individual stakeholder assessment are strongly qualitative (Florida, The Rise of the Creative Class 2012).

The 3Ts stand for talent, technology, and tolerance. Each factor is essential to assess an ecosystem or contributor and to analyze the pain points, strengths, and weaknesses. Technology represents the available technologies and the openness to understand as well as undertake innovative programs. For the complete ecosystem, this factor can be measured in the number of patents per capita and the patent growth. For the individual stakeholder, it can be quantified in the spending on R&D for governments, media, entrepreneurs, and corporations as well as the relative number of technology funds for investors (Florida, The Rise of the Creative Class 2012; Berk and DeMarzo 2014).

Figure 5 illustrates the framework and classifies the region into three categories. The green groups represent a thriving future and competitive advantage for a local ecosystem. Orange stands for a mediocre community that still can identify potential shortcomings through this scheme. Red indicates that there is a lot to catch up in order to become a prospering entrepreneurial ecosystem even if some areas are well developed.

A talent embodies the human capital and the available knowledge. For the whole community, it can be measured by the number of people who work in the creative class (e.g., computer, life science, art occupation) in relation to the people of the working class (e.g., construction, production occupation). For the individual stakeholder, it can be compared considering key personnel data and the percentage of creative jobs within the organization (Florida, The Rise of the Creative Class 2012; European Startup Initiative (esi) 2016). Last but not least, tolerance (which) stands for the diversity, openness, and equality within an ecosystem. This parameter can be measured by the share of immigrants, artists, and gays actively participating in the community (Florida, The Rise of the Creative Class 2012).

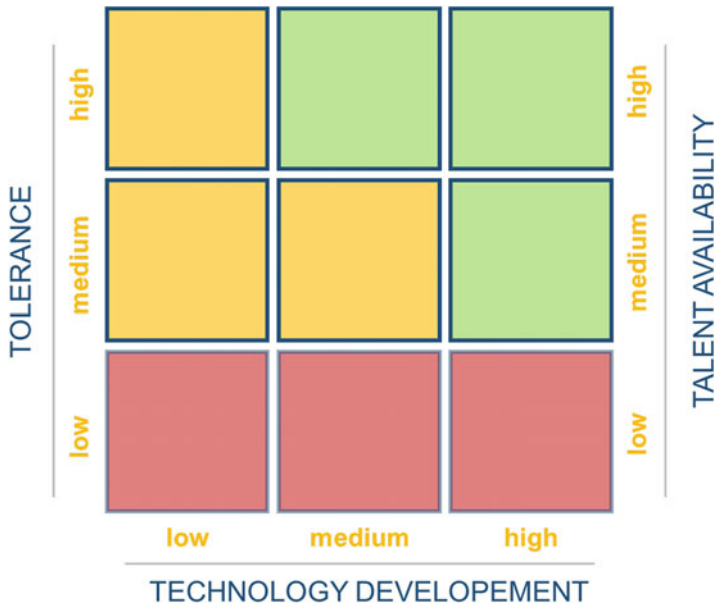


Fig. 5 3T framework in accordance with Florida (2012)

Conclusion

Startups have become a major force in today's economy. Entrepreneurs are compellingly passionate and drive new innovations and technology expeditiously. Startups can overcome entry barriers of key industries which were once believed to be unbridgeable such as automotive and consumer electronics through their purposeful hands-on approach to key technologic challenges. However, in most cases entrepreneurial ecosystems have not been able to react and respond to the startup phenomenon properly. Key hubs have been established, but several geographic areas failed to find their own success with technologic entrepreneurship.

First of all, administrations need to be aware of several key aspects and technologies that drive the information revolution. Network effects changed the way people communicate and connect to each other. The facilitation of assets has become the centerpiece of modern business. Industrial network-based systems allow startups to quickly innovate and disrupt industries through various partnerships with companies having specific expertise. However, there is an even more essential transformation concerning the social order. The rises of the creative class and creative jobs have changed the way we work, live, and interact in our daily life. The today's job requirements have changed significantly, and creativity seems to be the core part and the only human talent that cannot be replicated by a computer algorithm. In

order to cope with this phenomenon of a new workforce, it is essential to monitor social equality and the development of a clustered education singularity.

All stakeholders in the ecosystem like universities, investors, media, the government, and entrepreneurs are equally essential for the success of a local startup network. They must align and join forces in order to overcome the hurdles of the first years of technological pioneering. The seed stage is typically the most difficult stage in the startup life cycle, and entrepreneurs need providers to support their quest. Time, financial distress, and different core objectives of the contributors in the community can prevent an emerging local scene from being prosperous. However, startups are the clear leaders, and the other stakeholders represent the providers of the network. Each contributor must be self-aware of its function and needs to act accordingly.

To answer the research question how legislators and governments can improve the formation of startups and entrepreneurial ecosystems through political initiatives, administrations need to promote cyber development through entrepreneurial ecosystems. Knowledge and education are of major importance for startup success as well as the development of a knowledge economy, knowledge society, and knowledge democracy. Legislators should open the job market for international knowledge migration of tech talent. The formation of a knowledge state is a clear vision for an entrepreneurial ecosystem to be fruitful.

Eventually, the success of the startup ecosystem depends on three key principles: technology, talent, and tolerance. Firstly, foster the creation of knowledge and innovation throughout incentive research, universities, and interdisciplinary entrepreneurship. Secondly, invest in education and allow foreign people to frictionless participate in your community. Creative people are the centerpiece of successful innovations. And last but not least, create a diverse workforce, be inclusive to new contributors, and always try to change everything in your ecosystem. A clear for this is international knowledge migration.

For further discussion, I want to set up three propositions on how startup ecosystems can effectively improve the cyber development in a country. Through grants and initiatives in startups, the quality of democracy in a country can improve. Startups are positively improving HDI and GDP growth. A well-sounded entrepreneurial ecosystem progresses the sustainable development of a country's society significantly.

References

Airbnb, Inc. (2016). AirBnB. https://de.airbnb.com/about/about-us

Anders (a), G. (2014). Facebook's $19 billion craving, explained by Mark Zuckerberg. http://www.forbes.com/sites/georgeanders/2014/02/19/facebook-justifies-19-billion-by-awe-at-whatsapp-growth/. Retrieved 03 Aug 2014.

Anders (b), G. (2013). A twitter user is worth $110; Facebook's $98; LinkedIn's $93. *Forbes*.

Ashton, T. (1998). *The industrial revolution, 1760–1830*. Oxford: Oxford University.

Barnett, C. (2014). *Forbes magazine.* Top 10 crowdfunding sites for fundraising. Retrieved from: http://www.forbes.com/sites/chancebarnett/2013/05/08/top-10-crowdfunding-sites-for-fundraising/#53874f9e1cfb

Berglöf, E., & Perotti, E. (1994). The governance structure of the Japanese financial keiretsu. *Journal of Financial Economics, 36*(2), 259–284.

Berk, J., & DeMarzo, P. (2014). *Corporate finance* (3rd ed.). Harlow: Pearson Education Limited.

Block, J. H., Vries, G. D., Schumann, J. H., & Sandner, P. (2013). Trademarks and venture capital valuation. *Journal of Business Venturing, 29*(4), 2–18.

Campbell, D. F. J. (2013). *Cross-employment* (pp. 1–7). New York: Springer Science and Business Media, LLC.

Campbell, D. F. J., & Carayannis, E. G. (2016). The academic firm: A new design and redesign proposition for entrepreneurship in innovation-driven knowledge economy. *Journal of Innovation and Entrepreneurship, 5*, 12.

Chen, L. (2016, June 27). *Forbes*. At $68 billion valuation, Uber will be bigger than GM, Ford, and Honda. Retrieved from: http://www.forbes.com/sites/liyanchen/2015/12/04/at-68-billion-valuation-uber-will-be-bigger-than-gm-ford-and-honda/#1af9289d5858

Choi, J. (2016, August 11). *TechCrunch*. Google isn't safe from Yahoo's fate. Retrieved from: https://techcrunch.com/2016/08/11/google-isnt-safe-from-yahoos-fate/

Compass.co & Crunchbase. (2016). *Compass*. The global startup ecosystem ranking 2015. Retrieved from: http://startup-ecosystem.compass.co/ser2015/

Damodaran, A. (2015, January). Revenue multiples by sector (US). http://pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/psdata.html. Retrieved 09 Feb 2015.

Davenport, T. H., Harris, J. G., & Morison, R. (2010). *Analytics at work: Smarter decisions, better results*. Cambridge, MA: Harvard Business Press.

Dumont, B., & Holmes, P. (1999, October 25). The breadth of intellectual property rights and their interface with competition law and policy: Divergent paths to the same goal. *Financial Times*.

Dyer, J. H., Prashant, K., & Singh, H. (2004). When to ally and when to acquire. *Harvard Business Review, 82*(7–8), 108–115.

European Startup Initiative (ESI). (2016). *Startup heatmap.* Startup heatmap Europe. Retrieved from: http://www.startupheatmap.eu/assets/pdf/report_startupheatmap_europe_publish.pdf

Faccio, M., & Masulis, R. W. (2005). The choice of payment method in European mergers and acquisitions. *The Journal of Finance, 60*(3), 1345–1388.

Facebook, Inc. (b). (2014). Facebook investor relation stock. http://investor.fb.com/stockquote.cfm. Retrieved 02 July 2014.

Facebook, Inc. (c). (2014, October). FORM 8-K/A. http://investor.fb.com/secfiling.cfm?filingID=1326801-14-47&CIK=1326801. Retrieved 02 Nov 2014.

Feld, B. (2012). *Startup communities – Building an entrepreneurial ecosystem in your city.* Hoboken: Wiley.

Feld, B. (2015). *FeldThoughts*. What acquihire really means. Retrieved from: http://www.feld.com/archives/2015/07/acquihire-really-means.html

Florida, R. (2008). *Who's your city?* New York: Basic Books/Random House.

Florida, R. (2012). *The rise of the creative class*. New York: Basic Books.

Gompers, P., & Lerner, J. (2000). *The determinants of corporate venture capital success: Organizational structure, incentives, and complementarities*. Chicago: University of Chicago Press.

Gompers, P., & Lerner, J. (2002). *The venture capital cycle* (paperback ed.). Cambridge, MA: The MIT Press.

Graham, P. (2012, September). *Startup = Growth.* Want to start a startup? Retrieved from: http://www.paulgraham.com/growth.html

Haspeslagh, P. C., & Jemison, D. B. (1993). Managing acquisitions: Creating value through corporate renewal. *The Academy of Management Review, 18*(2), 370–416.

Jeng, L. A., & Wells, P. (2000). The determinants of venture capital funding: Evidence across countries. *Journal of Corporate Finance, 06*, 241–289.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons, 53*(1), 59–68.
Kaplan, S. N., & Stromberg, P. (2003). Financial contracting theory meets the real world: An empirical analysis of venture capital contracts. *Review of Economic Studies, 70*, 281–315.
Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2010). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons, 54*(3), 241–251.
Kuchler, H., & Bradshaw, T. (2014, February 20). Facebook buys WhatsApp in $19bn deal. *Financial Times*. http://www.ft.com/cms/s/0/44d4fc72-99b2-11e3-b3a2-00144feab7de.html#axzz366O3oTGA
Lerner, J. (2013). Corporate venturing. *Harvard Business Review, 91*(10), 86–94.
Levy, S. (2016). Facebook grows up. *The Founding Fathers of Silicon Valley, 1*, 68–79.
Mehr, H. (2016, August 18). *immobilienportale.com.* Zoomsquare: Facebook-Chatbot für die immobiliensuche. Retrieved from: https://www.immobilienportale.com/20165088-zoomsquare-facebook-chatbot-fuer-die-immobiliensuche/
iNiTS Universitäres Gründerservice Wien GmbH. (2016, August 14). *INiTS innovation into business*. Retrieved from: http://www.inits.at/
Opensource.org. (2016). *Opensource.org.* Coining “open source”. Retrieved from: https://opensource.org/history
Ries, E. (2010). *Startup lessons learned.* What is a startup? Retrieved from: http://www.startuplessonslearned.com/2010/06/what-is-startup.html
Robehmed, N. (2013, December 16). *Forbes magazine*. What is a Startup? Retrieved from: http://www.forbes.com/sites/natalierobehmed/2013/12/16/what-is-a-startup/#8f8336d4c63f
Roberts, B. (2006). *Show me the technology.* USA: Electronic Business.
Roland Berger & Pioneers. (2016). *Roland Berger.* Startup-Hub Wien. Retrieved from: http://www.rolandberger.at/presse/releases/Startup-Hub_Wien.html
Saxenian, A. (1996). *Regional advantage – Culture and competition in Silicon Valley and route 128*. Cambridge, MA: Harvard University Press.
Schlicht, M. (2016). *Chatbots magazine.* The complete beginner’s guide to chatbots. Retrieved from: https://chatbotsmagazine.com/the-complete-beginner-s-guide-to-chatbots-8280b7b906ca#.9ie4jua8l
Shapiro, C., & Varian, H. (1999). *Information rules: A strategic guide to the network economy*. Boston: Harvard Business School Press.
Sievers, S., Mokwa, C., & Keienburg, G. (2012, December 3). The relevance of financial versus non-financial information for the valuation of venture capital-backed firms. *European Accounting Review, 22*(3), 467–511.
TED Talks. (2015). *Ted.com.* The single biggest reason why startups succeed. Retrieved from: https://www.ted.com/talks/bill_gross_the_single_biggest_reason_why_startups_succeed
The Economist. (2014). *Facebook and WhatsApp: Getting the messages*. http://www.economist.com/news/business/21596966-why-mark-zuckerbergs-social-network-paying-such-whopping-sum-messaging. Retrieved 08 Aug 2014.
Uber Technologies Inc. (2016). *Uber*. Our story. Retrieved from: https://www.uber.com/our-story/
Vannevar, B. (1945). As we may think. *Atlantic Monthly, 176*, 112–124.
von Arnim, M. (2014). Das Ende der Internetblase 2.0. *Handelsblatt*. http://app.handelsblatt.com/finanzen/zertifikate/anlagestrategie-yahoo-aktie-profitiert-vom-boersengang/9912126-7.html
Waters, R., & Sharman, A. (2015, February). Google hopes all-or-nothing bet on robot cars will pay off soon. *Financial Times*.
Winkler, R., & MacMillan, D. (2016). *The wall street journal*. The secret math of Airbnb’s $24 billion valuation. Retrieved from: http://www.wsj.com/articles/the-secret-math-of-airbnbs-24-billion-valuation-1434568517
Yahoo! Corp. (2015). Yahoo finance database. http://finance.yahoo.com/. Retrieved 03 Jan 2015.

Cyber-Subsidiarity: Toward a Global Sustainable Information Society

13

José María Díaz-Nafría

Contents

Abstract

Most attempts to use the potentials of information technologies in benefit of the fulfillment of the democratic requirements from the local to the global levels are based on the power of social networks and the utilization of big-data approaches. However, both the network itself and the portliness of data processing have fundamental limitations that need to be overcome when the size of the population is larger than a reduced group. As to cope with the related complexity, the network provides in certain conditions a characteristic structure which facilitates the emergence of new functional features and consequently a system. It is this

J. M. Díaz-Nafría (✉)
Faculty of Systems and Telecommunications, Universidad Estatal Península de Santa Elena / SENESCYT - Prometeo, La Libertad, Provincia de Santa Elena, Ecuador

Faculty of Education, Universidad de León, Leon, Spain

Department of General and Interdisciplinary Studies, Munich University of Applied Sciences, Munich, Germany
e-mail: jdian@unileon.es

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_39

structure – the fibers of the systemic relations – and new functionalities concerning the circulation of data what change the portliness of data processing into an appropriate percolation and management of relevant information. By these means, complexity and the corresponding information flow are managed at the lowest possible level, while cooperation and higher-level management is ready to cope just with the excess of complexity the lower level cannot manage properly by itself. But this is the very idea of subsidiarity whose application to the organization of heterogeneous societies has been a foundation of decentralized government since the sixteenth century in many different contexts.

At the age of the global information society, the necessary management of global issues (environment, geopolitics, inequality, etc.) requires both proper levelism and information management from the peoples to communities, to national authorities, and to international institutions. Stafford Beer's Viable System Model provides a suitable approach to deploy subsidiarity with the backbone of an information and communication infrastructure based on the acquisition, circulation, and processing of relevant information to enable decentralized, democratic decision-making.

Keywords
Network theory · Semantic networks · Big-Data · Viable system model · Subsidiarity · Small-World · Cybernetics · Internet · Information divide · Biological information · Complexity management

Introduction

Imagine a kind of city constituted by a vast number of squares, where people meet and engage in different activities, but among which there is a scarce number of streets you can see. Some people move along them, but if you pay close attention, the number of people popping up or leaving each square are much more than the ones moving along the streets. We distinguish at the sides of the squares some doors through which lots of people pass through. The doors are guarded by watchmen who either let the people enter or not. It may be a sort of custom office, though it is difficult to see whether there is anyone charging. Some of these doors seem to be just for distinguished people – we guess – for whom the doors are opened when they intend to pass through, but there are other doors which are transited by the masses.

Considering the global flow, it is quite obvious that great avenues connecting the squares must be away from the eyes, but they have to be somewhere, surely underground. And indeed the people moving in that underworld must be tremendous, just by taking into account the large number of people in the squares with respect to the people moving along the visible streets. There is another clue to glimpse the complexity of such underworld: most of the people, before leaving one of these squares, go to a kind of small pavilion; seem to ask for something, and then, they go straightforward to some of the doors. Only in strange cases you get to see people going straight to the doors without passing by these pavilions. We presume it maybe the complexity of the underworld they are about to enter what make that people need to be informed. We also guess there is no cartography at hand about the underground streets, maybe it were too complex for human awareness. Although all that are mere conjectures we state from our bird-sight view of this weird city. Nevertheless, it is quite clear that there is no way to acknowledge the semblance of this city from any other one we have experience of.

Still many structural features of the social network geared by big-data technologies, as I will try to show, can actually be mapped in the ideal city we have just described. The latter serve as an allegorical approach to the ethical and political issues derived from the massive use of these technologies in all kinds of social activity and subsequently of the global information society (as the author has deal with in other works 2011, 2014). I say ethical issues because it concerns peoples' actions in their environments, their behaviors, affordances, and constraints. I mention political issues because it also concerns the collective decision-making. The previous picture has the benefit that, in contrast to the vast and multifarious complexity of the human activity mediated by the Internet, including all relevant infrastructural details, the reader have absolute control of the ideal city she has just depicted in her mind. This is analogous to the case of having a map in your hands with respect to the complexity of the territory, what by the way seem to be alien to the assets available in the weird city.

The question I intend to delve is: what is the most proper structure of the Global Information Society (GIS), including its infrastructural skeleton, as to cope democratically with the global complex issues we are facing? For many the answer to the proper way of dealing with these complex issues concerns precisely the big-data approach. However, I argue – in the vein of Stafford Beer and Norbert Wiener – that this is neither democratic nor the most effective way to face the complexity concerned. Nature and particularly living beings show us another way to face it. First of all, we need to see what the network in general properly is.

Abstract Networks, the Mapping of Complex Interactions, and Network Topology

A *network* in its naked flesh is nothing more than a set of *nodes* and *links* among them. It mathematically corresponds to a *graph*, namely, an ordered pair $G = \{V, E\}$ which comprises a set V of *vertices* or nodes together with a set E of *edges* or arcs. An edge is, in turn, a two-element subset of V (i.e., it is related to two vertices, being such relation represented as a pair which is usually ordered). In addition, both nodes and links have some arbitrary attributes (usually codified by labels or colors in the representation); but the most relevant feature for the node is its *degree*, k, namely, the number of links that connect it with the rest of the network, while for the link is its *directivity*, typically represented by an arrow (though links may also be bidirectional and then not represented explicitly). For the network altogether, it is the *degree distribution density*, $P(k)$ its most relevant attribute. These few elements of networks offer a sufficient flexibility to build a broad variety of models to map many real complex phenomena. (There are many introductory texts to network theory. Barabási (2002) has become a successful popular option, while van Steen (2010) and Newman (2010), among others, offer more technical details.)

When our network is mapping something in reality, the nodes (or the vertices in its representation) stand for some sort of *agency*. This can be either *active*, if the agent act by itself, or *passive*, if it is used by some active agent to perform the action. On the other hand, the links (or the edges) correspond to the *interactions* among agents. This correspondence is quite natural because whenever two real entities are somehow connected, they are actually interacting with each other. In order to have a broader spectrum of applicability, we may generally understand for agent whatever is capable of performing some action (either by itself or by other active agent) of any type (no matter whether it is of physical, chemical, biological, or social nature) (cf. Zimmermann 2012; Zimmermann and Díaz 2012; Díaz and Zimmermann 2013a, b). Therefore, what we represent through the network is a set of agents who operate onto other agents by means of their respective interaction.

Figure 1a illustrates a piece of network where the bidirectional interaction between two nodes, N_i and N_j, is highlighted. It is represented by the information exchange between the nodes, understood through a general and processual concept of information: N_i informs N_j, which comprises first a difference in the steady state of the connection, caused by N_i, and consecutively a difference produced in the state of N_j (it is straightforward to notice the alignment with Bateson's information concept, cf. Díaz-Nafría 2010). Thus we can speak of the information of N_i on N_j, i.e., $I_{i,j}$, and the information of N_j on N_i, i.e., $I_{j,i}$. The network as a whole represents synchronically all the interactions stablished among connected nodes. Figure 1b highlights the fact that interaction happens ultimately among agents. If we distinguish among active and passive agents, both graphs are actually not redundant: though active agents (we can take it as such Fig. 1b) may use passive ones (Fig. 1a), there is not a bijective relation between the corresponding components of both networks. Passive nodes can be used by several active ones, and, at the same time, several passive nodes may be required to provide the interaction between two active agents (telecommunication vs. communicators networks are clear examples to this respect).

The interaction represented by links can be regarded as *internal* for active agents and *external* for passive ones, since it requires the external intervention of some active agency. This is indeed a relevant difference that can be used to distinguish between the potential interaction of active agents – provided by the connectedness of the passive agents – and their actual interaction, provided by the "elections" of the active agents (we quote election to be aware that our agents can be of different

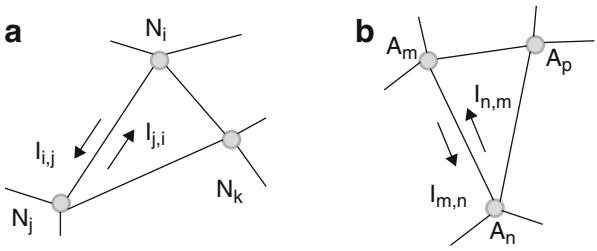


Fig. 1 Network as (**a**) set of nodes and links interacting with each other, (**b**) set of interacting agents

nature, thus it should not be interpreted anthropologically). Consequently whenever we just focus on a network of passive agents (a passive network), we are in fact dealing with the potentiality or space of possibilities in which the active agents perform their actions; whereas when we attend to the real interaction of active agents, it is the actuality within the former space of possibilities what is being represented thereby. In other words, when we map the network of active agency on the network of passive agency, we are observing the actualization of the potentialities represented by the passive network. The latter can then be seen as the space where the internal network (of active agents) is moving. This space can be understood as analogous to the phase space for the active network. Nevertheless, in the phase space (or space of possibilities of a system), each possible state corresponds to just one point, while here the active network is the result of all the external agents who are really active and occupy a subgraph of the passive network.

All in all, the static graph of the network – through this relation between potentiality and actuality of interaction – has the interesting property of representing motion. Indeed we can regard the physical space as a passive network of locations where the motion of physical entities takes place (by the way, different patterns of adjacency correspond in quantum gravity to different spatial geometries and consequently to different physical relations). A city composed by intersections and streets corresponds to the space where people move around. That is what we represented in the story we started this chapter with. But the passive network, as it is the matter of our concern, could also be the one composed by telecommunication lines and nodes which is the space where telecommunication among humans and machines takes place. These are the agents (nodes) of the active network we focus on.

Nevertheless, what the effects of the global interaction are depends significantly on the statistical and topological properties of the network, which are actually entangled. This is something we can realize observing the two most important network types (Barabási 2002): *random scaled* networks are highly homogeneous and distributed, while *scale-free* networks are heterogeneous having relatively common vertices with a degree that greatly exceeds the average. In the former type, the number of randomly distributed edges to be found is $p{\cdot}N{\cdot}(N\text{-}1)/2$, where p is the probability of one node to be bounded with another and N the total number of links. The grade distribution density, $P(k)$, for this type follows a Poisson law with a peak in the mean value, in which vicinity most cases arrange. However, in the scale-free networks the grade distribution follows a power law, $P(k) \sim k^{-\gamma}$ (where γ is typically in the range of $2 < \gamma < 3$). Here general network connectivity is guarantee by the hubs that concentrate a large number of links (interestingly major hubs are followed by smaller ones, which, in turn, are followed by others with an even smaller degree, and so on). Good examples for the first type are the vascular networks in animals and plants or the road networks of a country; while examples of the second kind are metabolic or semantic networks as well as air transportation networks. The second ones are considered scale-free because statistical and topographical features are reproduced when observed at different scales, i.e., they are *fractal*. They additionally provide an interesting topological feature making that networks of this kind constitute *small-worlds*, namely, that most nodes can be reached from every other

node by a small number of steps and, at the same time, that they have a large clustering coefficient (*C*: number of closed triplets/number of connected triplets of vertices; that is, nodes tend to create tightly knit groups) (Barabási 2002; Watts and Strogatz 1998).

Hence, most interaction in small-worlds happens at the level of clusters, while global connectivity is ensured with other clusters. Assuming structural stability (at least for a given observation window), we can state that whenever a cluster endures, this is because the interaction within the cluster corresponds to a proper issue management among cluster's agents; otherwise, the cluster would fall apart – looking for other effective interaction. In terms of information flow (which, as stated above, stands for interaction), the stability entails that the combined information in all directed loops within the cluster is convergent under issue management (otherwise issues would overwhelm cluster cooperation). In other terms, the complexity of the solutions against issues must be able to absorb the corresponding issues' complexity. In addition, information flow outside the cluster may correspond to the complexity excess not handled within the cluster but transported outside. Its amount is expected to be of a lower degree than the information flow within the cluster as a result of cluster's capacity to manage own issues.

Thus, clusters in stable small-world networks represent some effective cooperation. Subsequently, small-world networks seem to be well suited to instantiate the *subsidiarity principle*, namely, that issues are dealt with at the most immediate level that is consistent with their resolution. The additional requirements for the network structure needed to fulfill the subsidiarity principle is that only the interaction corresponding to issues that are better managed at the upper level percolate in that direction. In cybernetics jargon, this feature can be put in terms of Ashby's law of *requisite variety*, while Stafford Beer's Viable System Model offers the sufficient and necessary structural and functional requirements to enact subsidiarity and sustainability at the same time, as the author has argue elsewhere (Díaz-Nafría 2014, 2017). The aforementioned scale-free self-similarity, which is typical of small-world networks, has the counterpart in the recursive levelism which is characteristic of the viable system model.

On the Internet Topological and Structural Properties

Interestingly, when the very idea of the Internet was devised by Paul Baran (1964), it was the distributed topology that was born in mind as most appropriate to provide high resilience under attacks that could eventually affect critical nodes. That is, in fact, the quite obvious benefit for organism resilience provided by the distributed architecture of vascular networks. However, the self-organized evolution of the Internet has derived a decentralized topology which is instead scale-free. Indeed, its small-world property is illustrated by the fact that webpages, despite of being about five billions (Kunder 2016), are at an average shortest distance of only 20 clicks from any other one (assuming that such a path exists), according to the

estimative model provided by Barabási (2001). At the same time, the Internet infrastructure itself – constituted by a network of routers that navigate data packages for one terminal to another – is at an average minimal distance of some ten steps (*ibid*, Faloutsos et al. 1999). Both the Web and the Internet infrastructure are far away from the distributed topology, but still they provide significant robustness under random node failure (though critical nodes might severally affect global performance if they fail) at the same time that shortening network distance improves global performance significantly.

In the case of the Web, there is an interesting topological feature worth to describe, consequence of the highly heterogeneous linkage directivity: the Web breaks down in several well-identifiable continents (Barabási 2002): a *central core* in which each node is at reach of any other, an *IN continent* from which one can move into the core but not turning back, and an OUT continent where one can arrive but not come out; finally, there are *tubes* directly connecting the IN and OUT continents, *tendrils*, or node chains only attached to either the IN or the OUT continent, and a few nodes form isolated islands that cannot be accessed from the rest of the nodes. All this makes that robots that are tracking the Web to index have fundamental limitations to accomplish their task.

Figure 2 shows what can be taken as an image of the skeleton of the global information society (GIS), the Internet infrastructure expressed in terms of connected nodes (identified by IP addresses), though only for a part of it. According to the small-world properties, we can actually expect that the mapping of the whole Internet exhibits a similar structure. This topology offers at a time the potentiality to link any Internet node in a short time and the robustness of keeping overall performance before failures. However, is this actually all we need in order to provide connectiviness among two Internet (active) agents? If they know each other, they can exchange their addresses, and for that purpose, the Internet infrastructure provide the alleged potential, but this is not the general case for Internet agent interaction. These are often looking for contents or other agents to do things. As in the story we started with, "the complexity of the underworld they are about to enter [. . .] make that people need to be informed [about what venues they need to enter]". . . Here the big-data technologies enter the scene as an essential part of the Internet infrastructure.

However, there are still some issues regarding global connectiviness worth to be discussed. Figure 2 does not show the geographic distribution of nodes which are located for sure at the reach of some active agents. The very idea of the global information society assumes that everybody has the possibility to interact globally through the information infrastructure. But as Fig. 3 shows us this is not at all the case. The majority of world's population is still actually offline, as shown in Fig. 3a. Looking at the expanded information provided in Fig. 3b, we can notice that the geographic distribution of the – so to speak – offline continent is mostly located in the so-called developing countries. Something we can also observe in Fig. 4. Here global access inequality is clearly represented, but in comparison to income inequality, it seems to be lesser acute, though just in terms of bare connectiviness, which is of course a primary condition. Indeed, the qualification of the information society

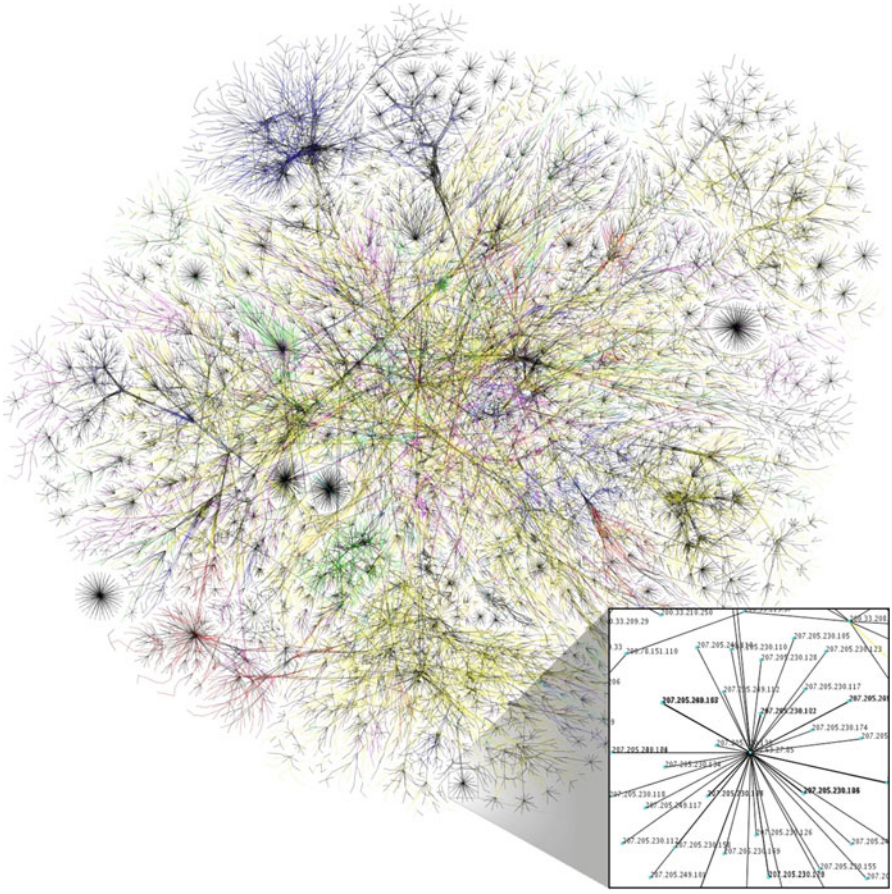


Fig. 2 Small look at the backbone of the Internet, actually less than 30% of the Class C networks reachable by the data collection program in early 2005. Each line is drawn between two nodes, representing two IP addresses. The length of the lines is indicative of the delay between those two nodes. Lines are color-coded according to their corresponding RFC 1918 allocation as follows: *yellow*, net, ca, and us; *magenta*, com and org; *light blue*, mil, gov, and edu; *blue*, jp, cn, tw, au, and de; *green*, uk, it, pl, and fr; *dark blue*, br, kr, and nl; *black*, unknown (Source: English Wikipedia)

depends on what is ultimately done online, and this depends, in turn, on who can actually operate digitally. If many people is left aside, online social life will not be so important. Indeed a critical mass is needed to make online life locally relevant, since it can effectively dealt with social issues.

In short, if the global information society is to be inclusive, then the primary condition is to have global online coverage. Although we are not in that situation, one can argue that, according to the trend of the ICT service evolution with respect to other basic services in the arguably called developing countries (shown in Fig. 5), there is a reachable horizon of global accessibility. In that respect, we can consider

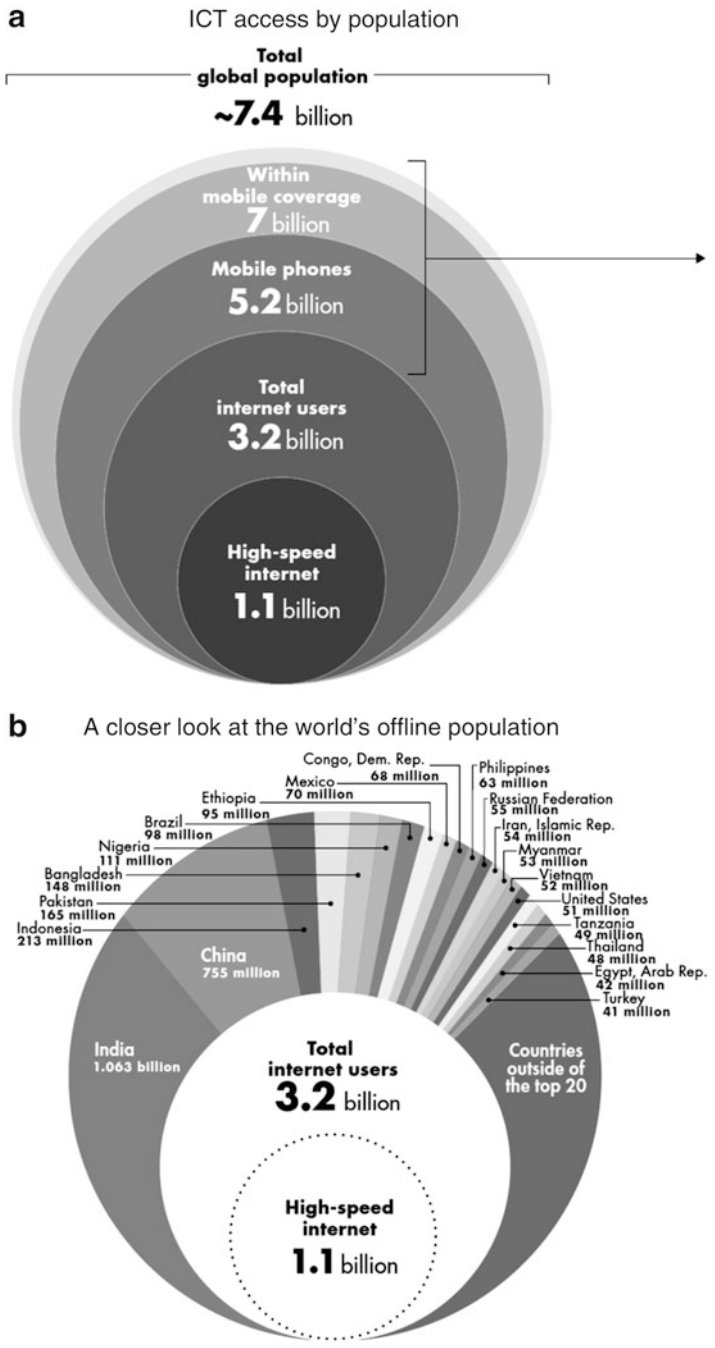


Fig. 3 ICT access by population. High-speed access is restricted to just the 15% of the population, while Internet remains unavailable, inaccessible, and unaffordable to a majority of the world's population (Source: World Bank 2016, License: Creative Commons Attribution CC BY 3.0 IGO)

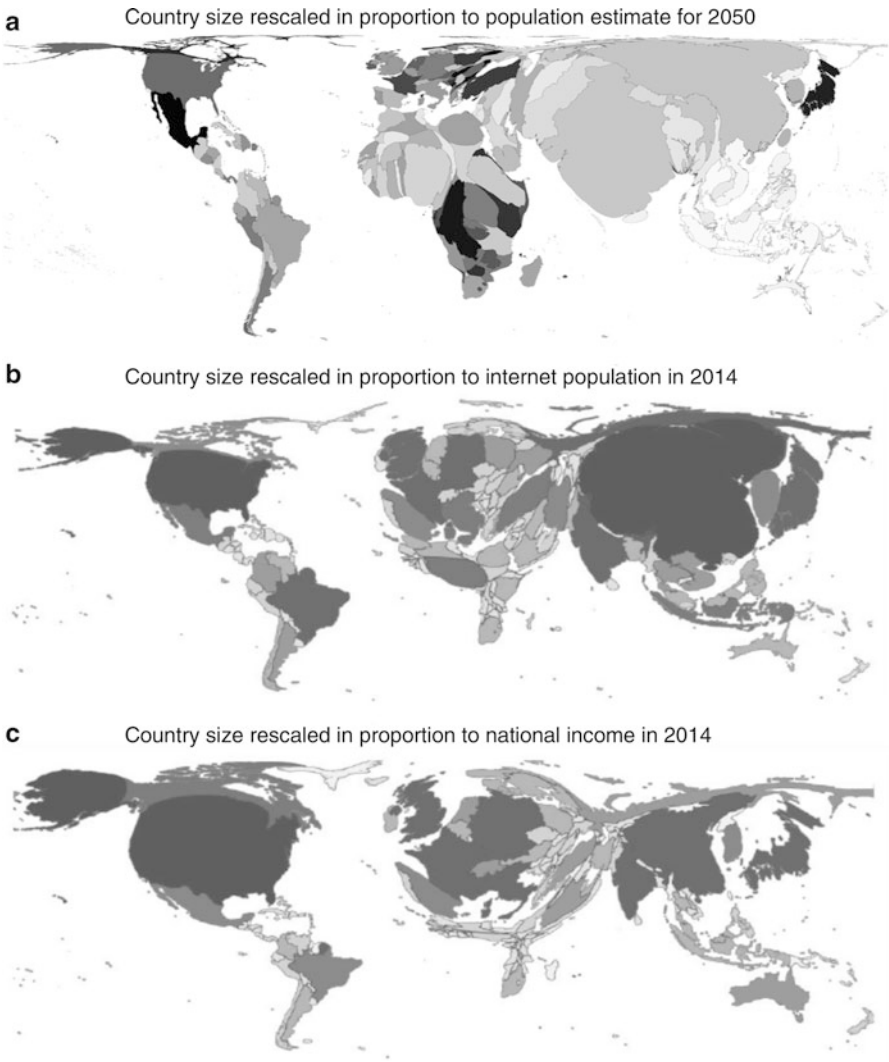


Fig. 4 The Internet is not worldwide distributed as population (comparison between **a** and **b**) but nevertheless more evenly spread than income (comparison between **b** and **c**). Country's size is rescaled in proportion to total and Internet population and national income. In (**a**), different tones correspond to dissimilar population growth; In (**b**), the darker the shade, the higher the Internet population; In (**c**), the darker the shadow, the higher the national income (Sources: World Bank 2016, CC BY 3.0 IGO; worldmapper.org, CC BY-NC-ND 3.0)

that in order to provide a proper skeleton for the global information society, it is not only bare connectivity but the structural properties of the linking infrastructure as a whole, which also includes the technologies facilitating the finding of proper connections, than matters in the end.

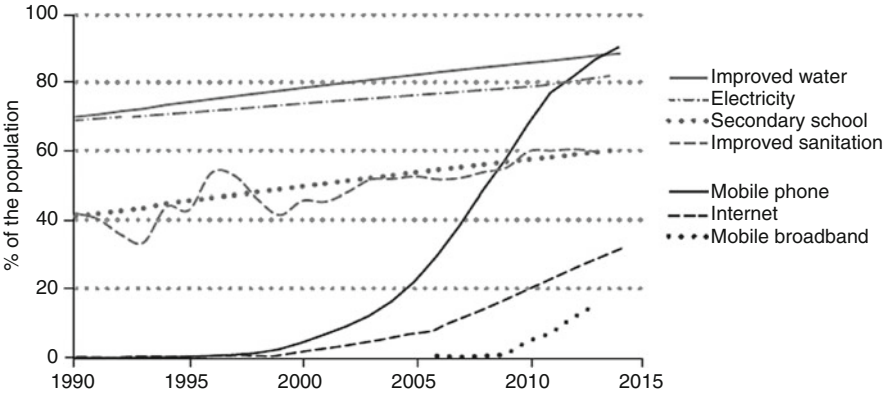


Fig. 5 The rapid spreading of digital technologies in developing countries (Source: World Bank 2016, CC BY 3.0 IGO)

Qualifying Connectiviness or How Good the Ties Must Be to Be Really Linked

Connectiviness is not all we need to know in order to qualify the value of the interaction among agents, as argued above. *Bandwidth* determines the space of possibilities of the interaction (how much one can affect another), *asymmetry* drives role distribution among actors and the share in decision-making, and *offline likelihood* affects trustworthiness severely and therefore what is ultimately done online. Moreover, the latter will always be paired with the offline activities, i.e., if essential agents cannot reliably operate online (due to either lack of connection or insufficient quality), the interaction carried out digitally will be shadowed. This is, of course, a major issue of the alleged global information society aligned to mere global connectiviness. In that respect neither the relative good news derived from Fig. 4 or from Fig. 5 are enough.

Therefore, beyond bare connectivity (which represents that some Internet interaction is just feasible), it is also important to inquire:

(Q1) The quality of such connectivity in terms of the probability that a link between two arbitrary nodes fulfills some minimal requirements to perform proper interaction, $p(Q_{Ii,j} > \text{threshold})$
(Q2) The probability to find the adequate Internet peer or resource

Ability to Operate Online

With respect to Q1, the Internet infrastructure composed by nodes and telecommunication pipes is decisive. Since *bandwidth* and *connection stability* are typically

aligned, we can mainly focus on the former. Figure 6 shows us that telecommunication lines are extremely concentrated in high-income countries. The distribution of this basic infrastructure actually follows approximately the real traffic telecommunication exchange distribution, due to the fact that in the past two decades new lines have been added following traffic demand very directly. Browning et al. (2012) display in more detail how both actual and potential traffic is highly concentrated in the connections among most busy nodes (London, Frankfort, Paris, Amsterdam, New York, Miami, etc., arranged according to 2012 global traffic data); in addition, we can observe that the regional density in Europe and North America with respect to other regions is even higher than income inequality, while peripheral regions, as Latin America or Africa, exchange even more with other regions that with themselves. This represents indeed an important breach in the subsidiarity principle we discussed above as a property that could eventually be at hand of the small-world structure exhibited by the internet architecture. How can this gap be closed? If the offer and demand of ICT resources is exclusively driven by monetary value, as it is in a substantial extent, the used approach to keep pace of customers' demand cannot suffice to satisfy peoples' demand unless there is a minimal equality among people's purchasing power, which is far from being the case. The problem is even worse if we consider that telecommunication rates are more expensive the further away you are from the economic center of the Internet (i.e., where more traffic is concentrated), due to the fact that the corresponding service provider is paying more expensive "transit" agreements to interconnect their networks. In sum, if subsidiarity is to be a regulatory principle of the global information society, then we should enact its positive sense to call for action at the higher level to enable that a minimal equality is guarantee (as a requirement for an inclusive information society) because at the lower level (with insufficient purchasing power) the problem cannot be solved.

A remarkable feature of user digital lines concerns its *asymmetric connection*, i.e., the inward versus outward bandwidth unbalance. That download bandwidth should be higher presupposes that information citizens are primarily consumers (as it is the case of ADSL connections). However from a network perspective, it must be a sort of balance among the overall interactions (i.e., information), particularly if under a sustainable horizon we admit some sort of metastability. Balance is breached just locally, at the global level producers must compensate what is being flown into consumers. If we group both kinds of agency, consumers on one side and producers on the other, information seem to flow mostly in one direction. However from the network perspective, information is after all an interaction that is compensated. If the only compensation were monetary, the information flow clearly corresponds to the commodification of cultural assets, in its general anthropological sense, namely, solutions given to social issues of any kind (manufacturing goods, knowing the circumstance, producing beauty, etc.). But this process would extract the creation of information goods from the flesh that ultimately produces it in the end (Fleissner 2006).

Nonetheless, if we pay close attention to the current trends of digital capitalism, many subtle ways that uses the Internet infrastructures have been created during the last two decades to feed from the consumer side the productive pole: several big-data

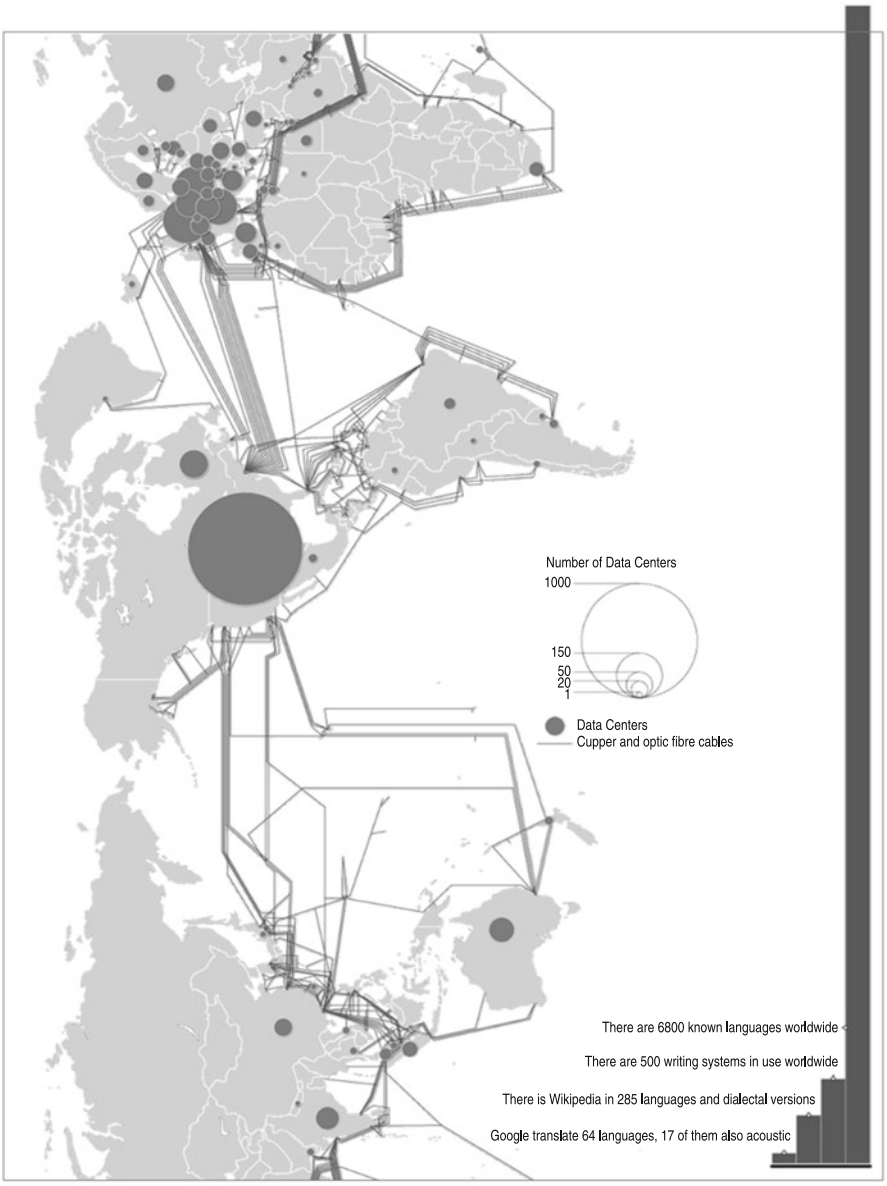


Fig. 6 Information pipes and data centers in 2012. Though the representation regarding telecommunication pipes is limited to overseas cables and its relative capacity is not represented, it can be observed that most communication pipes are concentrated among a limited number of nodes, mainly located in Europe and North America. Moreover, most information services as well as data and computing units available in the Internet are not within user devices but in high-security infrastructures connected at high-speed rates with other network nodes, known as data centers. How much these information services are represented in the language space is illustrated in the right bars, showing that the Internet sphere is dramatically exclusive (Source: Le Monde Diplomatique (2012), CC BY-NC 3.0)

technologies serve to this end, but there is a plethora of crowdsourcing techniques, among which Amazon Mechanical Turk is a good example, to illustrate the trend. Hardt and Negri (2009) characterize this process of global capitalism very clearly:

> "In the newly dominant forms of production that involve information, codes, knowledge, images, and affects, for example, producers increasingly require a high degree of freedom as well as open access to the common, especially in its social forms, such as communications networks, information banks, and cultural circuits. [. . .] The content of what is produced – including ideas, images, and affects – is easily reproduced and thus tends toward being common, strongly resisting all legal and economic efforts to privatize it or bring it under public control. The transition is already in process: contemporary capitalist production by addressing its own needs is opening up the possibility of and creating the bases for a social and economic order grounded in the common." (pp. ix–x)

Thus, through this process, in which capitalism is using people's creativity and work performance to cast the values, products, and services that providers put in the market, we are assisting to a detachment of human activity from people's problems or at least the way to dealt with them have stretched the loop, taking people's hands away from their own problems. Under the subsidiarity principle, the way to manage problems is the other way around. First people's hands have to be put on directly; thereafter, wider loops of the global net can get involved just to deal with the complexity excess. One direct consequence for an information society based on *cyber-subsidiarity* were a substantial decrease in long-distance information flow and the increase of the relative weight of the short-distance one. The overall flow of information would decrease dramatically – measured in bits per second moving along a meter, b·m/s. This is indeed the case of information management in living beings (Díaz-Nafría 2017): the shortest loops solve most issues through the corresponding information flow. Take, for instance, human motion: afferent and efferent neuronal information regulates "symmetrically" muscles' contraction to fit the coordinated actions of numerous muscular fibers to carry out a sophisticated cooperative action as regular walking. This flow circulates in a loop which is mostly closed at the level of the sympathetic neuronal network located in the spinal cord. Most information flows without any leak to higher network levels.

Ability to Find Resources and Peers

Regarding Q2, the finding of the proper resources or peers is certainly one of the highest concerns in ICT development during the last decades before the unprecedented increase of human capacity to store and to communicate information (represented in Fig. 7). Even though each user can be a powerful information producer, the required processing and data curation has been put in hands of a few *data centers* as illustrated in Fig. 6. Therein we can see how most information services as well as data and computing units available in the Internet are not within user devices, but allocated in high-security infrastructures connected at high-speed rates with other network nodes and highly geographically concentrated, known as

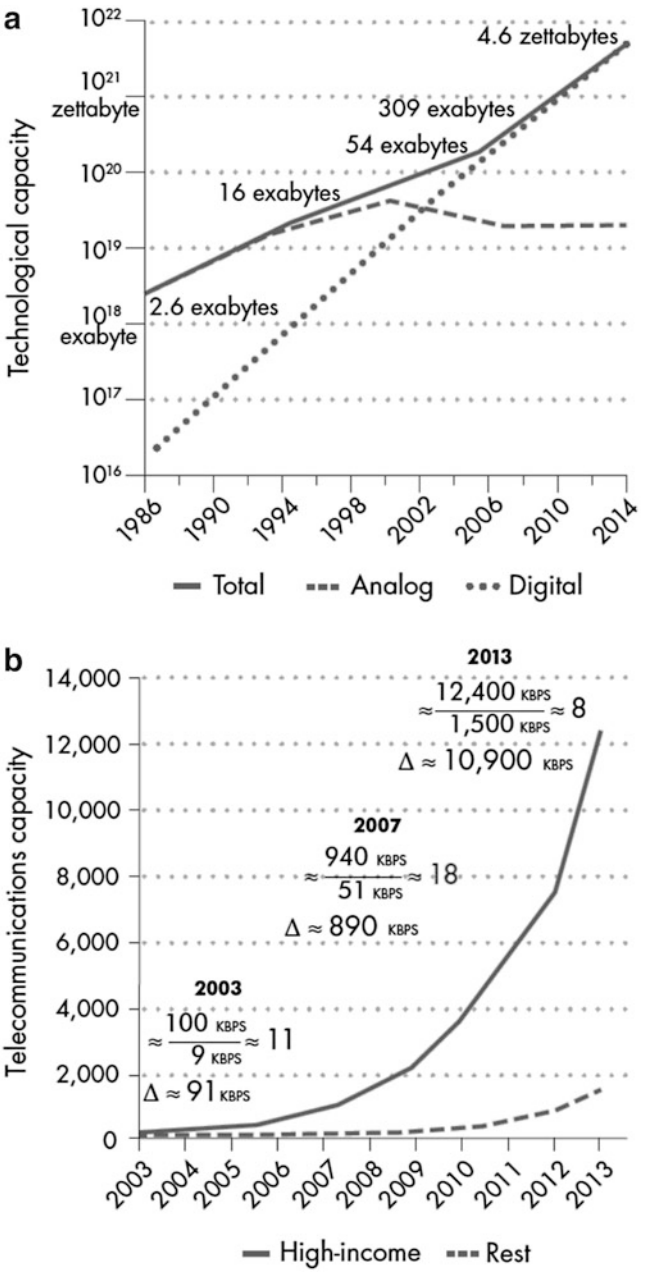


Fig. 7 Increase of human capacity to (**a**) store information and (**b**) to exchange digital information in high-income countries and in the rest of the world. In both cases, the figures considers optimally compressed information (Source: World Bank 2016, License: Creative Commons Attribution CC BY 3.0 IGO)

data centers which are geared by the big-data technologies. Its role in global economy, administration, and resolution of complex social and scientific issues has often been highlighted. Besides, the relevance of this – so to speak– guiding infrastructure is, for our inquiry, similar to the role of the pavilions located in the squares of the weird city of the introductory story: the unfathomable complexity of both the underground streets and the Internet backbone requires that the reach of proper nodes is assisted. Besides several alleged similarities, this situation is significantly different to what could be expected for the worldwide documentation system devised by Paul Otlet and Henri La Fontaine in 1910, Le Mundaneum. Such directory, actualized to today's World Wide Web content, instead of being centralized in Brussels, could be perfectly reproduced in anyone's computer, while the search for any resource we were interested in could be easily found using own computing resources. Right after, we could directly access the resource using the address provided by the directory – like the "people going straight to the doors without passing by [the] pavilions." The directory were somehow equivalent to the missing cartography of the underground streets.

From the structural point of view, the Internet geared by big-data technologies change in a substantial extent the effective structure of the Internet that we have discussed above and was illustrated in Fig. 2. In fact, whenever the interacting (active) agent requires big-data mediation, the corresponding network structure turns out to be highly centralized. On the other hand, the activity of the big-data agents is significantly alien to the subsidiarity principle: the bottom level (of data acquisition) is directly connected to the highest level (of storage, curation, analysis, and predictive processing) providing meaning affordances and constraints that are used in the making sense of the data which is ultimately top down oriented and used in benefit of some decision-making process (as far as we know, we cannot devise theoretically unbiased algorithms after all) (Cavanillas et al. 2016). There is no mediating upward-downward causation loop in between – closer to where the issues arise – which could contribute to the meaning extraction process. The data is collected massively, but the means to make sense of them are oriented by the need of extracting value from data, which necessarily adopt a top-down perspective. Nonetheless, according to the subsidiarity principle, this approach seems to be appropriate when dealing with global issues which in virtue of their complexity cannot be properly handled at a lower level. Indeed it offers a path to face many sustainable issues of the global information society, as global inequality, environmental issues, and the like, and therefore it may become a pillar to devise a sustainable information society (cf. Schwaninger 2015). The problem arises when instead of dealing with global issues the big-data approach is used to gain a competitive advantage when no minimal equality is guarantee. Since its ultimate usage concerns the enhancing of the decision-making, it is clear that an asymmetrical access to these technologies (significantly because of the necessary investment) drives to widening the gap among competitors and moving inclusiveness further away. On the other hand, letting aside intermediate subjects who are closer to the objects under study represents a significant loss in the understanding of problems and concerned reality and consequently a loss in the global problem-solving capacity.

But Fig. 6 shows us another relevant characteristic of the Internet infrastructure geared by big-data technologies with respect to its potential to become a sustainable global information society. The bars at the right side of the illustration show how big-data information services are represented in the language space. As we can observe, today's Internet sphere is dramatically exclusive: only 0.25% of the languages existing worldwide is acoustically available in the well-known translator resource offered by google, which could be naively seen as a tool for bridging cultural gaps. The relation between language and Internet is worth to be further explored to get a step ahead in our search for a sustainable information society. To this end, we will analyze from a network perspective what the language is for the corresponding community of speakers.

Lessons to Learn from the Semantic Network of Natural Language

In virtue of the centrality of language in the development of cultures in the broad sense and therefore in the human evolution with practical independence from genetic change, the corresponding semantic networks offer us valuable clues to rethink the architecture of the Internet infrastructure if it is to become the backbone of the alleged global information society.

A language can be mapped in terms of both a passive semantic network of linguistic elements and the active network of peoples who uses and drives language dynamics. The passive semantic network is constituted by the components of a language (words, syntactic, and semantic relations). Here the underlying infrastructure is constituted by the vocal tract of the speakers and the auditory system of the listeners together with the air that conveys the vibration generated by speakers toward listeners. This can be regarded as the passive network in which languages coevolve with a certain level of interaction.

At our level of abstraction, words (of a language) interact with each other passively. The speaker is needed. She puts them in interaction while making sentences. Through such interaction, namely, the relations established among the parts of the sentence, words mean something. Though they always mean it for someone (active agent) who is able to interpret it. Structurally, it holds a kind of democratic virtue: it practically offers to all language users the same space of potentiality, including the possibility to be directly connected to any other user. Figure 1a can be used to represent the network of words (where the directivity of links corresponds to predicative relations), while Fig. 1b represents the network of agents. They are connected to one another through the semantic network of linguistic interaction.

If we consider that speakers utter what is relevant for them, we can map relevance for a given population as the average of actual usage of the semantic network by such population, $R_p = E[\{R\}]$ (Fig. 8a). The dynamics of social relevance can then be mapped through the dynamics of the semantic network as actualized through the usage of each speaker (Fig. 8b). One can say that each speaker possesses a passive semantic network (acquired along her life) which is very similar to the ones held by

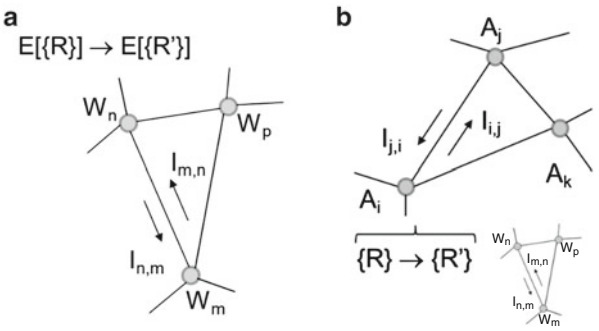


Fig. 8 Semantic network as (**a**) passive network of words (concepts) highlighted according to its relevance in social communication, (**b**) set of interacting agents

other speakers (lower part of Fig. 8b). The dynamics of her speech corresponds to the dynamics of what is relevant for her while immersed in a communication network. Thus, Fig. 8a stands for the average of the relevance dynamics represented in the lower part of Fig. 8b.

In contrast to the people linked through the existing Internet infrastructure, the community of speakers enjoys a space of possibilities (passive network), which is very equally distributed throughout the people and where the communicative acts can be developed. As we argued above, the Internet infrastructure offers a completely unequal space of possibilities for the deployment of social interaction.

Observing the semantic network in more detail, there is a central core of most used words which is shared by practically all speakers, at the same time that we can find clusters of words more connected to one another which are not so equally distributed. For instance, the vocabulary used to describe in detail living beings is mostly known by people associated to life sciences, and it is very tightly connected within words belonging to the same cluster; an even more specific vocabulary just dedicated to animals is more exhaustively known by zoologists. Since most issues related to a specific discipline are just dealt with among the people involved, the corresponding semantic cluster offers tight connections within itself and is shared by all the people involved. At the same time, enough connectivity is provided with the rest of the semantic network to deal with problems that require a broader intervention. Moving to a broader perspective, we observe language dynamics in permanent adaptation to cultural activities within their environments of evolution. For instance, inuits need referring to a large variety of snow types using different words, while other cultures do not need to be so specific. As we see, it is straightforward to notice that the semantic networks of natural language holds the subsidiarity property we have discussed above (see section "Abstract Networks, the Mapping of Complex Interactions and Network Topology").

Regarding the small-world properties, Sigman and Cecchi (2002) have found that for an extended vocabulary of 66,000 words, which includes domain specific terms, the average minimal distance between any two words is about 7. In addition, they found out that polysemic words and triangles (closed triplets) distributed all over the place seem to confer critical benefits. Polysemy offers shortcuts that tight the network effectively together. If we take them away, the average minimal distance

between arbitrary words turns out to be 11. Concerning triangles, when they start to appear during mother language acquisition, the learning process experiences an explosive growth which can be understood as a sort of emergence of the language ability (Corominas-Murtra et al. 2009). Interestingly during this transition, the semantic network acquires suddenly the small-world properties discussed in section "Abstract Networks, the Mapping of Complex Interactions and Network Topology," which enables the enacting of the subsidiarity principle in semantic development: child's language grows in permanent adaptation to the dealing with issues grouped in thematic clusters. These offers at a time a dense connection within domain vocabularies and a strong linkage to higher hubs (*ibid*). The enacting of subsidiarity can also be seen in terms of systemic emergence from the network: (i) initially the learner grasp a tree-like network of semantic connections that provides a basic linkage between herself and the things surrounding her in an activity language geared by a two-term syntax far away from adult language; (ii) the distance among terms and the vocabulary grows poorly clustered; and, (iii) within the critical transition the clustering grows, distance drops down, linkage and words increases; here the child turns to be able to utter adult-like syntactic structures characterized by its unlimited productivity. In other words, the system of language, able to refer our dealing with the surrounding world unlimitedly, emerges from the set of relations provided by the semantic network. Curiously, this unlimited productivity of language is determined by the *recursiveness* of natural language: the syntactic structures are built through a nesting process of substructures with no upper limit. Thus, as we have seen, recursiveness seems to be a fundamental feature of small-world networks, subsidiarity (see section "Abstract Networks, the Mapping of Complex Interactions and Network Topology"), and language.

Summarizing, there are several lessons we can learn in a network perspective from the semantic network of natural languages: (1) the language offers a passive network which is very equally distributed among language users; (2) language exhibits an evolutionary pattern adjusted to the subsidiarity principle which provides at a time flexible domain adaptation and global connectivity; (3) the semantic network of natural languages has small-world properties which seem to be fundamental to the enacting of subsidiarity; (4) the acquisition of natural language exhibits the sudden emergence of systemic properties driven by the qualitative transition of the network structure from star-like to small-world; and (5) the unlimited productivity of natural language rely on its recursive nature.

Lessons to Learn from Human body's Management of Information and Complexity

As illustrated in Fig. 7, human's capacity to store and exchange information has increased exponentially, and today's Internet seems to have an unprecedented size with respect to any previous collected information. This bulk, on the one hand, overwhelms individuals and, on the other, encourages corporations, governments, and international institutions that struggle to take advantage of it through the big-

data technologies as we discussed above. However, if we compare this tremendous information volume with the amount of information that is actually managed in the human body, the apparent giant becomes certainly small. Only the expression of the DNA (which information content amounts about 10^9 bits) to produce the cells contained in your body (about 4×10^{13} among which most of them have been replaced many times over) corresponds to an information amount much larger than what in Fig. 7 was termed as "human capacity to store information" (Milo and Phillips 2015). And we have omitted that for the development of many physiological structures like the nervous, or the immunological systems (and of course the bacteria we carry on, which are even more than our own cells), the information provided by DNA is completely insufficient. In addition, the information flow that is being managed in the body is definitely broadband. For instance, only the replacement of the red blood cells requires a flow of some 10^{16} b/s. Besides, there are lots of information corresponding to regulatory, metabolic, and productive interaction at the level of the cells and below. Before all this information flow circulating in ourselves is not astonishing that we can quietly contemplate a beautiful sunset?

The key for this quietness in the contemplation of the sunset relies on the physiological architecture of our organism which enacts as we will see the subsidiarity principle. In fact, Stafford Beer (1981) devised his viable system model, which corresponds to a systematization of subsidiarity, from the observation of the information and complexity management in the human body. Let us see Beer's analysis of the human organism. According to him, human body can be seen as primarily composed by three interacting parts: (i) the muscles and organs, (ii) the nervous system, and (iii) the external environment. The first part is being concerned with the primary activities, i.e., the basic interactions with the environment, and it is regarded as a solidary network of *operational units*. The second part ensures that the operational units (muscles and organs) work in an integrated, harmonic manner and can therefore be regarded as a *metasystem* (with respect to the system of operational units). And finally the *environment* refers to the parts of the outside world directly relevant to the organism, namely, in direct interaction with it – be it immediately or in the foreseen future (see Fig. 9).

Though the three parts are dynamic, there is a balance among them whenever the organism is in a sane situation. This means that the three parts are constantly adapting upon each other: (i) the muscles and organs adapt in a way or another in relation to the physical interactions with the outside, the metabolic activities, and the constant exchange with the nervous system; (ii) the neuronal and mental processes performed to regulate the organism, its activities, and metabolism conforms the constant adaptation of the nervous system in relation to the sensing interactions with the outer and inner environments, as argued above and elsewhere (Díaz-Nafría and Zimmermann 2013a, b); and (iii) the environment is similarly adapting according to organism's activities (for instance, some living beings run away, some others cooperate, and others play against).

The articulation of the human's nervous system, as proposed by Beer (1981), is particularly relevant to understand his model for the management of information and

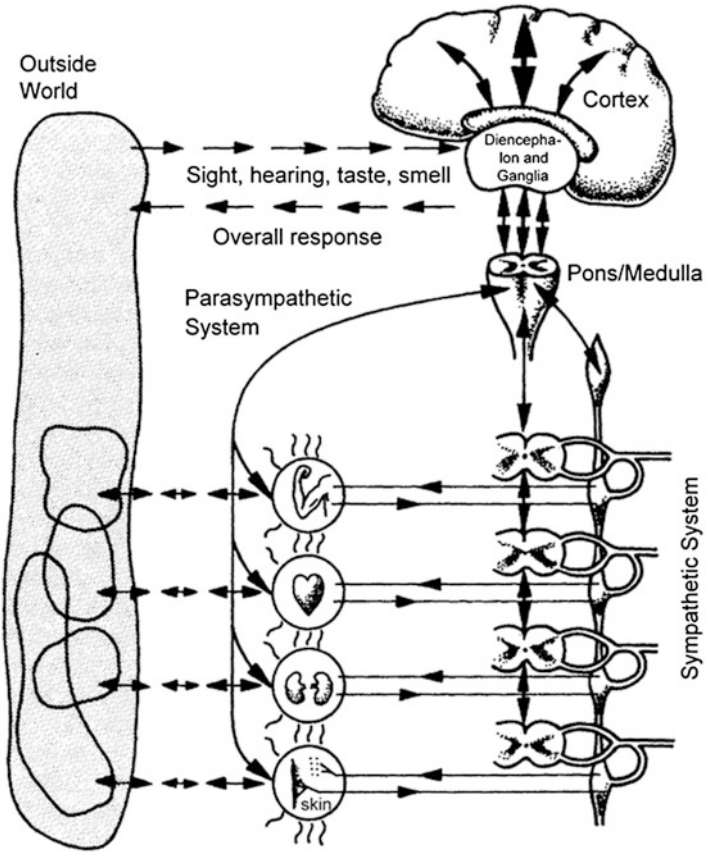


Fig. 9 The human organism from Stafford Beer's cybernetic perspective can be regarded as being primarily composed by (i) operational units (muscles and organs) inscribed by circles; (ii) the nervous system which in turn is composed by the sympathetic system, the base brain, the diencephalon, and ganglia and the cortex; and (iii) the environment (Illustration elaborated from Beer (1981, p. 131))

complexity. He distinguishes four systems in tight connection with the operational units which constitute what he calls *system 1*, namely:

System (2). The sympathetic nervous system which stabilizes and coordinates the activity of muscles and organs through the resolution of conflicts

System (3). The base brain, including pons, medulla, and the parasympathetic system, which enables internal regulation and optimization

System (4). Composed by the diencephalon and ganglia, linked to the outer senses and committed to the forward planning

System (5). The cortex which regards the higher brain functions performing self-identity, ultimate decision-making, and axiological orientation

If we now consider the information management, the first lesson learned shows us that most information actually circulates at the level of system 1, particularly if we include therein the afferent–efferent pathways closed by the interneurons in the spinal cord. Second, the existence of other pathways through the sympathetic trunk shows the possibility to regulate through information exchange with the higher nervous system, but in most cases this only embraces system 2 for the short-term coordination of organ activity or system 3 if longer term coordination is required. Indeed, a very small fraction of regulatory information reaches system 5 as proven by the fact that the bandwidth of conscious awareness is in the range of only 100 b/s or less, while, in contrast, the bandwidth of the information managed in the retina is about 6×10^6 b/s (Anderson et al. 2005; Norretranders 1998).

We can still move to a lower level to observe, for instance, that the simple contraction of a muscle fiber corresponds, at the level of the cell, to a number of metabolic interactions among the constitutive parts of the fiber which complexity is higher than the afferent/efferent exchange to regulate the contraction. And we can go even deeper if we focus on the inner activity of the subcellular organelles within the eukaryote cell. Whenever we deepen an additional level, the overall information flow at the lower level is larger. Toward higher instances, few information percolates.

This reduction of information flow from the lower to the higher regulatory bodies corresponds to a distributed and autonomous management of operational complexity and simultaneously the percolation of only the mostly relevant with respect to the dynamics of the whole. Thereby, if one is grabbing a flower, most of the information flow to regulate the complex coordination of muscle fibers will only circulate at the lowest level, in which the corresponding network of synapsis has "learned" how to do it, but if in the movement one is acutely pricked by a thorn, the information of the pain stimulus will circulate all the way up as to make – all the way down – the whole body to escape from the danger (Beer named this type of percolation as *algedonic,* stablishing a symbolic relation to pain, *ἄλγος*, and pleasure, *ἡδονή*).

All in all, the biological management of information shows us that it is possible an intense alleviation of information flow and the coping with a maximal complexity, thanks to a proper hierarchical architecture (or rather heterarchical as we have just seen) composed at each level by a network of relatively autonomous agents, whose cooperative actions are oriented to the resolution of issues at the lowest possible level, and the coordination of actions among the parts. This architecture clearly endorses the subsidiarity principle, offering additional clues to cope with global complexity in the information society. Therefore, we take it as the model for cyber-subsidiarity.

In comparison to the big-data approach discussed in section "Qualifying Connectiviness or How Good the Ties Must Be to Be Really Linked," we observe here that information only percolates if it becomes relevant for the overall operation' therefore, value is directly guarantee in benefit of a more appropriate decision-making. By these means, the whole is able to coordinate action according to what is most relevant for the present and future adaptation to the environment, therefore guaranteeing sustainability of the whole and the parts.

Cyber-Subsidiarity as a Backbone of the Global Information Society

Whereas the social order arisen with modernity encompassed – at the level of the nation-states – a reduction of social complexity through cultural normalization, the new social and political order is nowadays, as a consequence of globalization, to be intercultural, multilingual and even multinational. National life is more and more entangled with international relations and cannot be conceived anymore with our backs turned to intercultural populations and to nature. All this makes that the traditional context of posing ethical questions is rather different. The universality paradigm that pervaded many classical approaches in ethics is not so convincing anymore, and ethics and politics become more entangled than ever. Anthropology, ethnography, and intercultural ethics has shown the fragility of such pretentious positions whose social and political correlate is bureaucracy. The realm of goals is fixed therein, and the effective pathway to achieve them seems to be at reach of its rational determination. The efficiency of this paradigm for the organization of the industrial enterprise and the state has been indeed a decisive factor for the extension of its power. Just the rational determination of means implies a substantial reduction of complexity driving to an efficient performance of the prescribed actions and goals. Observe that the praiseworthy precursor of the big-data data approach corresponds to the gathering and processing of statistical data for the organization of the bureaucratic state and enterprises since the eighteenth century and it was within this endeavor where the computing and information technologies were pushed forward (Mattelart 2003).

As we discussed in section "Qualifying Connectiviness or How Good the Ties Must Be to Be Really Linked" regarding big data, the upward flow of data to the center, where the meaning and value is produced, as well as the downward flow of its application evades the conscious intervention of the intermediary agents and therefore the participation of the peoples in the decision-making. If this is the case, are not we reproducing through the big-data technologies the bureaucratic approach to a magnified scale? When we have confirmed that this organizational paradigm accumulates unsolved problems, we must encounter a different way of diminishing the complexity at the level of the human agency and all the way up to the global scale. Is not possible to make sense of information and computing technologies in a direct assistance of human autonomy and in benefit of people's democratic participation while looking for a global sustainable horizon?

Let us see whether the fulfillment of democratic sustainability is actually feasible from the local to the global scales, considering an account of democracy beyond the common nominal use of the term, in the vein of *qualitative democracy,* particularly as conceived by the *Quadruple Helix* model (Campbell et al. 2015). Democracy since its Greek roots is conceived as linked to both equality and liberty (In Aristotle, these principles are aligned with the ethical virtues which in turn stem from the very human nature; cf. Aristotle 2004, VI, 2): equality with respect to the capacity to decide upon available common options and liberty with respect to the self-determination or autonomy of the community members, who should not depend

on some authority in order to make really free choices. Equality thus concerns the right to participate equally (social value), but it also entails that a minimal satisfaction of needs is provided as to ensure real autonomy (material value). Therefore, concerning material equity, democracy admits a certain degree of inequality, but this is strictly bounded by the need to guarantee autonomy (Post 2003). As it has been proven, though democratization can be achieved under inequality conditions, in the long term, it undermines the consolidation of democracy (Houle 2009), and moreover, it is correlated to the decrease of democratic political engagement (Solt 2008). This relation has even been stated by the OECD in the report concerning public engagement: "Decision-making is founded on broad participation and equality of citizens" (OECD 2009, p. 146). As we saw in section "On the Internet Topological and Structural Properties" (Fig. 4c), the global information society is far away from such situation.

In historical perspective, it can be observed indeed that despite the constantly growing global inequality since the eighteenth century (measured for instance through the Gini coefficient), the localized reduction of inequality has often been associated to democratic processes, as in Western Europe, where the strengthening of social security systems improved the autonomy of the citizens during the decades following World War II (Milanovic 2009). But since the 1980s, we observe within these countries a general increase of national inequality, as well as between EU countries, which provides a clue to the often highlighted EU democratic deficits (Díaz-Nafría 2014; Díaz-Nafría et al. 2015).

To this respect, it is remarkable to recall that, though the *principle of subsidiarity* was first proposed in the context of the early Calvinism, it was the striking increase of inequality in the early industrialized societies what brought the principle to the fore of sociopolitical concern. In the XVI century, Althusius developed the concept in the milieu of the Calvinism communities immersed in a Catholic empire as to preserve their autonomy while enabling symbiotic relations with the larger society. However, in the industrialized areas of the nineteenth-century Europe, it was the dramatic increase of observed inequality and the subsequent arisen contradiction between work and capital that made evident the undermined autonomy of the many and consequently the inability to accomplish the principles of democratic liberalism. In this context, the principle of subsidiarity was developed and incorporated into the sociopolitical agenda (Nell-Breuning 1990). It progressively became a fundamental principle of democratic liberalism and a pillar of the Catholic Church social doctrine, and it is now one of the foundations of the EU, who has coded the principle as a pillar of the Union itself (EU 2008: art.5). Internationally the principle has been coded as a foundation of decentralization and co-responsibility (UN 2014), and it has been even devised as a core concept for the organization of complex systems (for instance, in the field of neuropsychology and cybernetics). This is in fact what underlays the aforementioned organization of organisms devised by Stafford Beer in his search of the principles of any sustainable organization.

Hitherto, this understanding of subsidiarity requires moving beyond the *negative account* of subsidiarity (as it has been extensively done in the EU in order to prevent action of public bodies) and developing instead a *positive strive* by public

institutions to act where no other closer instrument is actually acting as to ensure fundamental rights.

As we can observe in Stafford Beer's Designing Freedom (1974), his positions clearly stand for the development of a completely new way of making sense of computing and telecommunication capacity as a means to overcome the bureaucratic paradigm in the benefit of both deploying freedom and the coping with complexity. By these means, he envisions a reconciliation of ethical and political action superseding the limitations of the liberal ethics and the bureaucratic organization of economic and political life. As we saw above, he learned from biology the lesson of how to deal with complexity, deriving the fundamental and necessary structure depicted in Fig. 10 that any viable system – able to constantly adapt to its environment – should hold (Beer 1981). The functionality of Systems 1–5 is the direct correlates of the ones described in section "Lessons to Learn from Human Body's Management of Information and Complexity," in short: *System (1*) autonomous and mutually adaptive operative units, *System (2*) coordination and conflict management, *System (3*) strategic planning and optimization, *System (3**) auditing of System 1 performance, *System (4*) long-term planning, and *System (5*) ethos and normative management.

The model relies on two fundamental principles (Beer 1981): (i) *Ashby's law of requisite variety* and (ii) the principle of *recursiveness*. According to the first principle, the capacity of System 1 has to be balanced with the framework of operations that it assumes, leaving a sufficient leeway and guaranteeing that the only variety (complexity) left corresponds to what is better achieved at a higher cooperation level. The recursiveness is an obligated counterpart of the former principle in order to distribute the coping with a complexity which is much higher than what a reduced number of autonomous agents can perform. Downward, the levelism stops at the agency that is taken as the model of sustainability (namely, the human), but upward it is in principle unbounded. We can symbolically express the recursive structure of the VSM as

$$\mathrm{VSM} \stackrel{\mathrm{def}}{=} \{\{\mathrm{S1}\}, M|\mathrm{S1} \stackrel{\mathrm{def}}{=} \mathrm{VSM};\ \mathrm{M} \stackrel{\mathrm{def}}{=} \{\mathrm{S2},\ \mathrm{S3},\ \mathrm{S3}^*,\ \mathrm{S4}, \mathrm{S5}\}\}$$

Similar to the unlimited productivity of the language, argued in section "Lessons to Learn from the Semantic Network of Natural Language," this property enables its application to an unlimited complexity, which management comports the devising of appropriate information channels (as illustrated in Fig. 10). The success of this architecture has been shown in several organizations, but the most astonishing experiment is undoubtedly its implementation at the level of Chile's state by Allende's government of popular unity through the utilization of very simple but effective electronic means (Medina 2012). This had the objective to connect people's issues and decisions at the lowest but most notorious level with state management at the highest, through an appropriate levelism in which relevant information (and particularly the algedonic one) percolates from one level to the next. Nevertheless, though this was the target of the Cybersyn project, the implementation just achieved the management of the nationalized economic companies between 1972 and 1973.

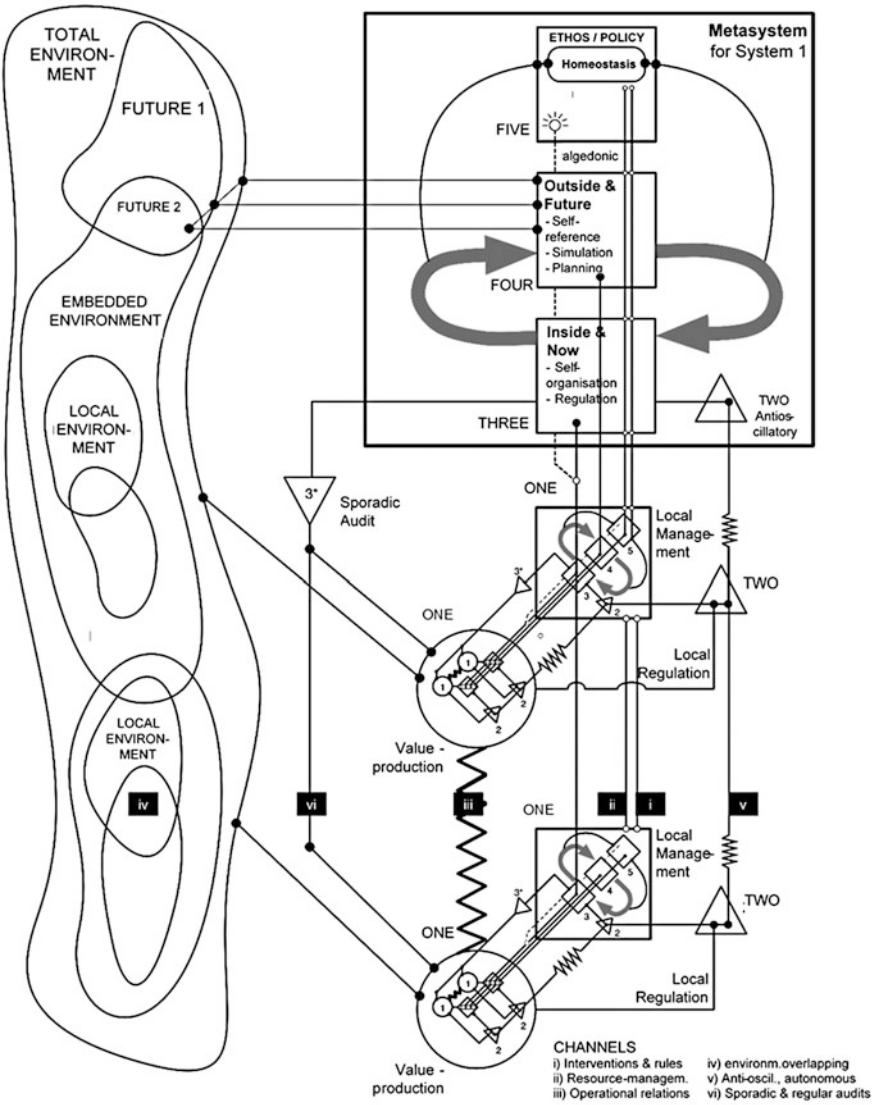


Fig. 10 Stafford Beer's Viable System Model (cyber-subsidiarity) for any sustainable organization. Its recursiveness is explicitly represented in System 1. System 3* correspond to an extension of System 3 to enhance its knowledge about System 1 performance in order to provide a better regulation. (Illustration elaborated from Lambertz (2016))

Such economic control proved its strengths against the soft power (referring to the distinction coined and advocated by Joseph Nye (2004)) supporting Allende's opposition and organizing two massive transport strikes, but it brutally collapsed under the bombs of the hard power in the other black 9/11th of 1973 (Díaz-Nafría

2011; Medina 2012). The case is of significant interest, on the one hand, because it addresses at a time the question of developing individual liberty and the coping with global issues and, on the other hand, because it has been extensively documented particularly since Medina's book (2012; Beer 1975, 1981). Nevertheless, despite Allende's strong concern of furthering radical democracy in an efficient way, it must be born in mind its direct connection to nation–state political economy and how the leeway of the latter has significantly changed since as argued above. Fortunately, the scalability of the organizational core model of subsidiarity, stemming from its recursiveness, is capable to address the additional complexification that should be dealt with in order to handle *cyber-subsidiarity* at a global scale, which is in fact the level that is needed to enact sustainability properly (Díaz-Nafría 2011; Díaz-Nafría et al. 2015; Schwaninger 2015).

Conclusive Remark

Looked through the glass of the *Quadruple Helix* model (Campbell et al. 2015), we can easily observe that the cyber-subsidiarity model provides sound means for the development of qualitative democracy at the global information society in its four dimensions, namely, freedom, equality, control, and sustainability. Consequently, the cyber-subsidiarity model serves as a regulatory account to boost a decent global information society, particularly concerning the requirements that the global information infrastructure, discussed above, should meet. With respect to the structural requirements of the links connecting the parts of the cyber-subsidiarity model (Fig. 10), it is quite clear that the backbone of the global information society critically analyzed in sections "On the Internet Topological and Structural Properties" and "Qualifying Connectiviness or How Good the Ties Must Be to Be Really Linked" lacks significant components. First, the positive account of subsidiarity has to be strongly claimed as to achieve a proper universal coverage in terms of an equalized capacity to operate. Second, the information that should percolate from the links belonging to clusters at a given level (arranged in operational networks) to the higher level is just information that is relevant to the operation of the higher level (frequently obtained as nonlinear aggregates), while the information concerned with the issues attached to an specific cluster is just shared within the cluster. By these means, a proper control is provided from the lower levels to the higher ones (through accountability and participation), and at the same time autonomy is preserved, sustainability fostered (through responsibility and adaptability), and information flow significantly alleviated. Third, forecasting capacity should be placed not at the highest level, as in the big-data model, but distributed throughout the different scales from the local to the global. This enables a distributed tackling of global issues and subsequently a substantial alleviation of what is to be dealt at the global level, and at the same time general sustainability is achieved in virtue of an enhanced adaptation capacity at all levels of concern.

The structural similarity between the small-world (and scale-free) network exhibited by the Internet backbone, and the cyber-subsidiarity model, offers a

convergent path for the development of the later. The evolutionary benefits of the scale-free networks in terms of trustworthy connectivity and robustness, as observed in linguistic or biological networks, are worth to be keep, but not to the expense of the necessity that they supposed to be responding to. Namely, the connectivity of all peoples with an equalized capacity to operate. However, if the market, driven by financial capacities, keeps on offering the basic mechanism to the deployment of the Internet, this can never suffice to meet the objective unless a minimal equality is achieved. Consequently, a global and conscious endeavor – not driven by the market – to boost cyber-subsidiarity would offer the double-faced benefit of promoting global qualitative democracy (including the four dimensions mentioned above) and rationalizing the development and costs of the ICT infrastructures (alleviating the global information flow – as observed in the organisms, section "Lessons to Learn from Human Body's Management of Information and Complexity," – and shaving the huge investments devoted to the big-data projects).

In contrast to the weird city we depicted at the beginning, in an allegorical city corresponding to the cyber-subsidiarity model, we would not see the small pavilions used by the people before leaving the squares; the visible streets between near squares would be mostly populated; some squares were highly connected to others in each quartiers and these to others of the city center. Probably it could also be hard to acknowledge the semblance of this city from any other one we have experience of, but just considering the fact that the people seem to be able to move around by their own, we have the feeling that this must be a better place to live.

References

Anderson, C. H., et al. (2005). Directed visual attention and the dynamic control of information flow. In L. Itti, et al. (Eds.), *Neurobiology of attention* (pp. 11–17). San Diego, CA: Elsevier.

Aristotle. (2004). Politics: a treatise on Government. Trad. In W. Ellis (Eds.), Gutenberg Project. http://www.gutenberg.org/ebooks/6762 Accessed 20 Aug 2016.

Barabási, A. (2001). The physics of the web. *Physics World, 14*(7), 33–38.

Barabási, A. (2002). *Linked: The new science of networks*. Cambridge, MA: Perseus Publishing.

Baran, P. (1964). *On distributed communications: I. Introduction to distributed communications networks*. Santa Monica: RAND Corporation. http://www.rand.org/pubs/research_memoranda/RM3420.html. Also available in print form. Accessed 15 Aug 2016

Beer, S. (1975). *Designing freedom*. New York: Wiley.

Beer, S. (1981). Brain of the firm. 2, Wiley, UK.

Browning, N., Krisetya, M., Lairson, L., & Mauldin, A. (2012). *Global Internet Map 2012*. TeleGeography. http://global-internet-map-2012.telegeography.com/. Accessed 10 Aug 2016.

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493.

Cavanillas, J. M., Curry, E., & Wahlster, W. (Eds.). (2016). *New horizons for a data-driven economy: A roadmap for usage and exploitation of big data in Europe*. Basel: Springer.

Corominas-Murtra, B., Valverde, S., & Solé, R. (2009). The ontogeny of scale-free syntax networks: Phase transitions in early language acquisition. *Advances in Complex Systems, 12*, 371–392.

de Kunder, M. (2016). The size of the World Wide Web (The Internet). WorldWideWebSize.com: http://www.worldwidewebsize.com/. Accessed 15 Aug 2016.

Díaz-Nafría, J. M. (2010). What is information? A multidimensional concern. *TripleC, 8*(1), 77–108.
Díaz-Nafría, J. M. (2011). The need for an informational systems approach to security. *Triple C, 9*(1), 93–121.
Díaz-Nafría, J. M. (2014). Ethics at the age of information. *Systema: connecting matter, life, culture and technology, 3*(2), 43–52.
Díaz-Nafría, J. M. (2017). E-subsidiarity: An ethical approach for living in complexity. In W. Hofkirchner & M. Burgin (Eds.), *The future information society: Social and technological problems*. Singapore: World Scientific Publishing.
Díaz-Nafría, J. M., & Zimmermann, R. (2013a). Emergence and evolution of meaning. *Triple C, 11* (1), 13–35.
Díaz-Nafría, J. M., & Zimmermann, R. (2013b). The emergence and evolution of meaning. The GDI revisiting programme. Part 2: Regressive perspective. *Information, 4*(2), 240–261.
Díaz-Nafría, J. M., Alfonso, J., & Panizo, L. (2015). Building up eParticipatory decision-making from the local to the global scale. Study case at the European higher education area. *Computers in Human Behavior, 47*, 26–41.
EU (European Union). (2008). Treaty on European Union and the treaty on the functioning of the European Union. *Official Journal C*, *115*, 1–388. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=OJ:C:2008:115:TOC. Accessed 10 Aug 2016.
Faloutsos, M., Faloutsos, P., & Faloutsos C. (1999). On power-law relationships of the Internet topology. *ACM SIGCOMM Computer Communication Review, 29*, 251ss. ACM S/GC0MM 99.
Fleissner, P. (2006). Commodification, information, value and profit. *Poiesis & Praxis: International Journal of Technology Assessment and Ethics of Science, 4*(1), 39–53. doi:10.1007/s10202-005-0007-y. Accessed 22 Aug 2016.
Hardt, M., & Negri, A. (2009). *Commonwealth*. Cambridge, MA: Cambridge University Press.
Houle, C. (2009). Inequality and democracy: Why inequality harms consolidation but does not affect democratization. *World Politics, 61*(04), 589–622.
Lambertz, M. (2016). *Freiheit und verantwortung für intelligente organisationen*. Düsseldorf: Mark Lambertz.
Le Diplomatique, M. (Ed.). (2012). *Atlas der Globalisierung – Die Welt von morgen*. Berlin: Le Monde Diplomatique-Deutsche Ausgabe.
Mattelart, A. (2003). *The information society: An introduction*. Thousand Oaks: Sage.
Medina, E. (2012). *Cybernetic revolutionaries: Technology and politics in Allende's Chile*. Cambridge, MA: MIT Press.
Milanovic, B. (2009). Global inequality and the global inequality extraction ratio. The story of the past two Centuries. *Policy research working paper 5044*. World Bank – Development Research Group.
Milo, R., & Phillips, R. (2015). *Cell biology by the numbers*. New York: Garland Science.
Newman, M. (2010). *Networks: An introduction*. Oxford: Oxford University Press.
Norretranders, T. (1998). *The user illusion*. New York: Viking.
Nye, J. S. (2004). *Soft power. The ways to success in world politics*. New York: Public Affairs.
OECD. (2009). *Focus on citizens: Public engagement for better policy and services*. Paris: OCDE Publishing.
Post, R. (2003). Democracy and equality. *The Annals of the American Academy of Political and Social Science, 603*, 24–36.
Schwaninger, M. (2015). Organizing for sustainability: A cybernetic concept for sustainable renewal. *Kybernetes, 44*(67), 935–954.
Sigman, M., & Cecci, G. A. (2002). Global organization of the Wordnet lexicon. *Proceedings of the National Academy of Sciences, 99*, 1742–1747.
Solt, F. (2008). Economic inequality and democratic political engagement. *American Journal of Political Science, 52*(1), 48–60.
UN. (2014). *Global governance and global rules for development in the post-2015 era*. United Nations. http://www.un.org/en/development/desa/policy/cdp/cdp_publications/2014cdppolicynote.pdf. Accessed 12 Aug 2016.
van Steen, M. (2010). *Graph theory and complex networks*. Twente: Marteen van Steen.

von Nell-Breuning, O. (1990). *Baugesetze der Gesellschaft*. Freiburg: Solidarität und Subsidiarität.
Watts, D.J.; Strogatz, S.H. (1998). Collective dynamics of 'small-world' networks. *Nature,* 393: 440–442. doi:10.1038/30918. Accessed 15 Aug 2016
World Bank. (2016). *World development report 2016: Digital dividends*. Washington, DC: World Bank. doi:10.1596/978-1-4648-0671-1.
Zimmermann, R. E. (2012). An integral perspective of social action: Imagining, assessing, choosing (onto-epistemology of networks). *International Review of Information Ethics, 18*, 221–236.
Zimmermann, R., & Díaz, J. M. (2012). The emergence and evolution of meaning. The GDI revisiting programme. Part 1: Progressive perspective. *Information, 3*(3), 472–503.

Libya: Where Cyber-Democracy Reached Its Limits – How the Case of Libya Challenges the Idea of Cyber-Development

14

Nathalie Hoffmeister and David F. J. Campbell

Contents

N. Hoffmeister (✉)
Department of Political Science, University of Vienna, Vienna, Austria
e-mail: nathalie.hoffmeister@gmx.de

D. F. J. Campbell
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (Iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@aau.at; david.campbell@uni-ak.ac.at; david.campbell@univie.ac.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_54

Abstract

Blessed and at the same time cursed by the availability and presence of natural resources (African fossil energies), Libya has always constituted to be of a particular interest for the West. Due to the largely underdeveloped and rudimentary Internet use, and with a barely existing shared identity that would contribute to a sense of nationality, the Libyan people were unprepared at the beginning of the Arab Spring in 2011. Unlike the Tunisian counterpart and example, Libya does not have a strong diaspora in Europe that would show an attachment to Western values and commodities. In addition, the fact that the former authoritarian regime in Libya operated an anti-Western and nationalist policy, everything associated with the West was commonly being disregarded. Even if Libya's authoritarian regime was in no way inferior to those in its Arab neighbors, the momentum and result of the Western intervention in 2011, is to be seen primarily as an indication that a sustainable democratic consolidation, to which a cyber-development and cyber-democracy should contribute to, is being seriously challenged. Therefore, this work attempts to show the drawbacks of cyber-democracy by using Libya as a negative example. It should be argued that cyber technology is only conducive to and supportive for democratic tendencies if this is also being wanted by the users (the users of democracy). What is necessary is to lead Libya out of its present misery that is being produced by two (if not even three) competing governments and by radical jihadist aspirations that are tearing apart and fragmenting the entire society. Finally, possible solutions for problem-solving will be explored, also being framed in various "thought experiments" (scenarios), also with regard to premises and principles of cyber-development and cyber-democracy.

Keywords

Algeria · Arab Spring · Civil war · Crude oil · Cyber-Democracy · Cyber-Development · Democracy Potential · Libya · Political Transition · State Consolidation · Thought Experiment · Tunisia

Introduction

> Technology is neither good nor bad; nor is it neutral. (Kranzberg 1986)

Inspired by the idea of cyber-democracy as a phenomenon, which under certain conditions may contribute to advances and progress in democracy and democracy results, and the actuality that such a phenomenon is commonly associated with the Arab Spring, especially in Tunisia and Egypt, this work would like to concentrate on the Libyan case by exploring why the revolution could (or did not) not succeed there (so far).

It is often being assumed that the Maghreb states or the North African states are more or less similar concerning their socio-demographic or even cultural and historical background. Nevertheless, it cannot be said in any way that in Libya something other than a tragedy has taken place, while in Tunisia and Egypt, a transition to a consolidated democracy is slowly and certainly yet to be established (with an outcome much more open in Egypt after the de facto military intervention).

So where are the differences in these supposedly similar countries? To sum it up, all the countries were authoritarian regimes and they were mainly being secured by a strong military force. Set aside that Libya happened to be the sole Arab-Spring-country where the United Nations intervened, it was clear from the outset that the Yasmine revolution would not be continued. Therefore, this work should, after careful consideration of the peculiarities of the Libyan state with its (political) history and with a closer look at the phenomenon of ICT (Information Communication Technologies) possibilities and options, show that such technologies are usually only sufficient for the promotion of democracy only when intended to do so (Xavier and Campbell 2014). Furthermore, it should be pointed out that in the special case of Libya, there were completely different challenges that alone could not have been overcome with ICT. Inevitably, one could anticipate that a society striving for democracy, which is networked and mobilized via the Internet, can still not counter a military attack. In addition, when comparing the mobilization dynamic, which was cohesive in the Tunisian case, unquestionably one has to regard a nonaligned Libyan nation in this instance. Last but not least, it should be recalled that "democracy" is a well-conceived concept, oriented mainly to the standards of the West; it is increasingly overlooked that democracy can have several appearances, especially when considering that these states are still in an embryonic stage. Since this work has to limit its scope, the focus will be on the year of 2011, in order to highlight where and why the decisive moments of a democracy consolidation were missed or even ignored.

Therefore, this work is carried out hypothetically and mildly illustrates the current developments in Libya, since the attention is to be put on the supposedly missed democracy potential. However, the extent to which Libya can be transformed and reformed is to be finally explored in a "thought experiment" (scenario development) toward the end of our analysis.

The Oddity of Libya's Founding

A Symbolic Gift to the Arabic World

After the founding of Israel in 1948, the founding of Libya must be interpreted as a "gift to the Arab world" by the United Nations – a proud Arab monarchy, which should let resurge the Arabian dignity. The real struggle for independence came in 1969, when Gadhafi overthrew the monarchy. The Colonel turned out to be a corrupt dictator, who formed alliances with different tribes, thus securing his power. This tribal culture has not yet been dismantled, and the present lines of conflict are between the tribes, rebels, and cities, fighting over power; in part, they are ideological conflicts as well, irrespective of the rich oil reserves of the country.

Unlike its North African neighbors, it had no unified independence war during the decolonization phase, as this was the case for example in Algeria.

> Alors qu'en Algérie, en Tunisie et dans une large mesure au Maroc, les relations tribales et la culture tribale ont décliné pour être remplacées par des liens de classes, des relations partisanes, voire des liens de patronage, le cas libyen diffère alors même qu'il y a développement de la population urbaine; il y a persistence de la culture tribale, en particulier de la culture politique de la statelessness – du non-État ou du sans-État – et par là de l'image of statelessness, de la représentation du non-État. (Djaziri 2009 p.130–131)

Libya was, and still is, a region divided into three parts – The Kyrenaika, Fessan, and Tripolitania, where various tribes reside. The tribe serves as an identification tool; the nationality "Libyan" was presumably only relevant on paper.

> D'autre part il fallait s'appuyer sur les liens de parenté et sur les réseaux tribaux pour gouverner une société qui résistait à toute unification. (Djaziri 2009, p.129–130)

Ironically, Colonel Gadhafi seemed to be the solely vital link in the Libyan society not only due to his charismatic and exaggerated appearance. Everything was associated with him and his reign so that after the coup, the Libyan people disaggregated deeper in tribal and ethnic rivalries, which over the years had been constrained through Gadhafi's affiliation politics. The only unifying momentum and aim was to topple him. As soon as this was achieved, a situation arose where every single tribe and rebel group tried to raise their profile and position themselves in the most effective way. Therefore, the so-called starting position for a nation to rise further into its own state and to rearrange political order was accompanied by local clashes and no real unity was unfolding (Haimzadeh 2015).

Gadhafi's Jamahiriya: Neopatrimonialism in Its Purest Form

The self-immolation of Mohammed Bouazizi on December 17, 2010, which triggered the Arab Spring in Tunisia, is to be rated partially as a symbol of the subsistence economy, as it is being found in many places in Africa. It is characterized by the circumstance that it is not one's singular aim to gain profit, but just to ensure the survival of one's family. This is due to the arbitrary corruption of the regime, which makes sustainable economic planning impossible. On that momentous day, Bouazizi could not bear his desperation over the local officials anymore and resulted in him taking his own life. Similar to its North African neighbors, Libya's population is rather young and unemployed. Therefore, the profound aspiration for change is chiefly shared by every young man and woman in that region.

This phenomenon is significantly rooted in the tradition of neopatrimonialism. Marked by a highly personalized state administration and policy, and often controlled by a powerful loyal military staff, neopatrimonialism does indeed feature a legal bureaucracy – but parallel to this, it is undermined by the unpredictability caused by the arbitrary power of the ruler. Gero Erdmann states that:

> The patrimonial system of personal relationships, and the legal-rational system of bureaucracy, with the patrimonial system encroaching on the legal-rational one and deforming its functional logic and effect [...] Informal policies have reached such a dimension that is has to be labelled institutionalized informality, which is at the same time an institutionalized uncertainty (translation of author) (Erdmann 2002, p. 334)

Associated to this, Gadhafi owned tremendously loyal private paramilitary entourages, which is also known as a neopatrimonialism feature (which will be issued in greater detail in the following analysis).

Especially during the 1970s and 1980s, he pursued a merely pan-Africanistic and pan-Arabistic policy, ideologically charged through *The Green Book*, and isolated his own people from Western influences. Moreover, we assume that a barely remarkable Libyan diaspora living in the Western world or Europe is not crucial enough to introduce the Libyan people to western customs as it would be the case in Tunisia with its key sector in tourism and a deep linkage with its former motherland France; set aside the fact that Libya was an Italian colony and might have a noteworthy diaspora there, actually no close connection revealed itself. In addition, Libya is rich in oil spills, so it never had to become a holiday destination, which can be observed in Tunisia.

> No genuine industrial development occurred outside of the petroleum sector – and even there, the oil slump of the 1980s cut Libyan revenues dramatically. (Brahimi 2011, p. 608)

Differences Between the Tunisian and Libyan Military

In General

> Common ethnic, tribal, and secretarian identities are often seen as the most reliable indicators of loyalty, and regimes can reduce the chances of military dissent by staffing their armed forces with these 'communities of trust'. Finally, authoritarian rulers create multiple layers of intelligence agencies and paramilitary institutions, whose job is to monitor the regular armed forces and defend the regime against the military in case of a coup attempt. (Makara 2016, p. 213)

The military in Tunisia, as well as in Egypt, was very institutionalized – unlike in Libya, where Colonel Gadhafi occupied his military staff according to tribal affiliations.

As Florence Gaub pointed out, the military force in Tunisia has to be seen as a professional representation of the Tunisian *state*, whereas the Libyan armed force was noncohesive allied to the *regime*. These two parameters already indicate fundamental differences.

Historically seen, the relationship between the military forces in Libya and the regime was always quite ambivalent, particular with regard to King Idris and his mistrust against the military, since this was a symbol of a modern state, "which he viewed with suspicion" (Gaub 2013, p. 225). This wariness continued existing in the Gadhafi regime where the Colonel had to balance out his ambivalent bond with the

military "in a way that allowed for maximum regime support while at the same time limited its actual capacity in order to curtail its power" (Gaub 2013, p. 227). This ended in the circumstance that Gadhafi kept surrounding himself with a special loyal paramilitary force ("Revolutionary Guard corps") under his direct control, while simultaneously weakening the regular armed force systematically through so-called coup-proofing (Gaub 2013, p. 236). "When put to test, such as in Chad or during the uprising of 2011, the Libyan armed forces' cohesion proved to be feeble" (Gaub 2013, p. 232). This was not the case in Tunisia; although both Ben Ali and Gadhafi graduated from military services, Ben Ali never became the charismatic Colonel Gadhafi used to be. It was the whole Ben Ali family who were notorious for its corrupt and greedy affairs. Supposing that the Tunisian military did not necessarily rely on Ben Ali's favor, as observed in Libya where the military career was depending on tribal and ethnic heritage, a strong affiliation between the president and the military was absent.

> In Tunisia, Ben Ali's Presidential Guard was the sole beneficiary of the regime's patronage distribution [. . .] Indeed, whereas militaries are often symbols of national pride, Ben Ali treated his military as a second-class citizen. Illustrating the military's inferiority is the fact that it, along with other security personnel, had to be searched by the Presidential Guard before receiving permission to protect Ben Ali's family. (Makara 2016, p. 218)

During 2011

> Indeed, this pronounced tribalism helps to explain the surprising resilience of the regime despite four decades of sustained brutality, a series of coup attempts, wasteful military campaigns, an unprecedented and widespread popular rebellion and a targeted NATO bombing campaign. Those who came to the regime's defence fought not only for their political and economic privileges but, necessarily, for their lives. (Brahimi 2011, p. 612)

Correctly stated above, the Libyan military burden was much more intense than it was in Tunisia. Therefore, the evidence that the military in Tunisia and Egypt refused to proceed against the protesters during the Yasmine revolution is easier to explain here:

> The fact that the military can be jointly responsible for and has played a decisive role that change took place peacefully in both countries [Tunisia and Egypt] is beyond question. (Schwarz 2012, p. 37)

> Thus what is correct in Egypt is not necessarily correct for another country. In Libya the situation necessitated entering into bloody battles and massacres of Libyans, given the 'tribal nature and geographic separation' that characterized the society [. . .] This nebulous and intricate tribal order interwoven with militias viewed the system as the state; where if the capital did not fall, then the authority could never be brought down. (al-Afifi 2012, p. 432)

Nevertheless the Libyan military was not the main actor during the Yasmine revolution in 2011 but so was the Revolutionary Guards and the Libyan police (and

special well-equipped brigades directly under Gadhafi or his sons). "In these units, loyalty to the regime and unit cohesion were almost identical features" (Gaub 2013, p. 233). But it still remains interesting to mention that defecting movements during the months of 2011 were drawn upon, among other criteria, tribal and ethnic lines; "the Libyan military had allegedly shrunk to somewhere between 10,000 and 20,000 (from its original 51,000)" (Gaub 2013, p. 235).

The Marginalization of His People

> In the 1970/1980s many developing countries feared the impact of new information technologies. Some dictatorships such as Libya required that all computers, telephones, fax machines and other communication devices be registered with the government. (Howard 2011, p. 57)

Moreover, the highly personalized system of Gadhafi, and further the decisive partitioning of a society toward the outside world, must be considered here additionally. Certainly, there are urbanization processes, especially in the big cities like Benghazi or Tripoli. Despite the voices as above mentioned, indicating a differed depiction, there is some indication that the Libyan population also made use of the digital age. "But in many developing countries, mobile phones and computers are shared resources, available for use by several family members and not discarded or replaced as quickly" (Howard 2011, p. 19). Hitherto one still must keep in mind that Libya is the worst performing country on digital networking and usage among its Arab neighbors.

> As for Libya is had one of the lowest Internet penetration rates in the Arab World. Adding to that, the Libyan civil society was being totally suffocated by the Qadhafi regime to the point where there was a total absence of cadres of grassroot movements that had the ability to mobilize the Libyan streets. (El-Nawawy and Khamis 2012)

> Indeed, early on, civil society was eradicated [...] The regime has shut down the institutions and places where people might gather outside government supervision, and the government launched a takeover of the media in 1980 [...] The regime confiscated and destroyed property, nationalised oil and land, and asserted the monopoly on imports and exports. (Brahimi 2011, p. 608).

From the period of his reign, Gadhafi accomplished to isolate his people from the public perception so that they became totally subservient and unheard. Therefore, a functioning internet access is not a guarantor for mobilizing a social movement. Gadhafi vehemently persecuted his political opponents (live streaming of hangings on TV and torture). Esther Turnhout describes in her article, "Heads in the clouds: knowledge democracy as a utopian dream", from the year 2010:

> However, the public is not a pre-existing entity waiting to be involved; it is brought into being-performed in the context of participation. Participatory initiatives are sites of power in the sense that they create their own participants in ways that fit with the objectives and expectations of the initiator. (Turnhout 2010, p. 8)

Here, it is already suggested that new technologies are, of course, an influencing factor when it comes to mass mobilization, but it is also necessary to examine who or what is behind this initiative and what it aims to achieve. "Thus, what is envisioned under the label knowledge democracy is not necessarily democratic" (Turnhout 2010, p. 35).

ICT Benefits for Extremist Groups

Hence, it is arguable that extremist groups such as ISIS ("Islamic State of Iraq and Syria", also being called ISIL, the "Islamic State of Iraq and the Levant") do also find great use in ICT concerning recruitment objectives and mobilization of potential followers. For a favorable western democratic mind, this even constitutes a clear form of abuse of cyber technology, which entails the need for further investigation to combat or even prevent this form of danger. From this viewpoint, the freely accessible Internet access, as it is praised in terms of cyber-democracy, is in this scenario rather counterproductive.

Furthermore, it is crucial to keep in mind that such groups evaded their domestic internet surveillance and restriction on Islamist tendencies on a large scale by forming a hideout in Europe, even perhaps the United States:

> Until 2011, Islamist ideas were shaped primarily in exile. Libyans even attribute the survival of the Islamists to their experiences in the West, where many came into contact with the ideas of the Muslim Brotherhood while students in the US and Europe. Islamist ideas were banned in Libya, where Qadhafi once compared the movement to a cancer. But they were freely accessed in the West. (Omar 2012, p. 49)

ICT as a Tool of Oppression

We can even take it a step further and postulate as it was indicated above that sophisticated ICTs might be degenerated by dictators, such as Gadhafi himself was, and become a tool of oppression:

> Several internet thugs were employed by the regime to monitor online activists and to launch Facebook pages and online campaigns to publicize for the regime. (El-Nawawy and Khamis 2012)

In this regard, the Libyan society had nothing left to oppose and were quite unable to put up a defense mechanism. As "Keren (2006) argued that online media alone cannot lead to concrete political action on the ground, because online activists could be helpless vis a vis the evil they experience or observe, and their helplessness is only marginally relieved by the sense of community that is emerging online [...] Feelings such as fear of oppression, resentment toward authority and vulnerability [...] are not easily reduced by online-writing" (El-Nawawy and Khamis 2012). Correspondingly, it is evident that not only the authoritarian government finds use in

the ICT sector, but also opponents or even extremist groups who want to counter the state or its government.

> Moreover, a set-theoretic explanation of the role of ICTs in contemporary democratization requires that we identify a consistent set of causal relations between technology diffusion and democratic outcomes. (Howard 2011, p. 28)

"Satellite news services have done much to help create a pan-Islamic identity [...], reconnecting diaspora communities with political events" (Howard 2011, p. 29), how it was the case during the Yasmine revolution in Tunisia, also "militaries, that find themselves disadvantaged both politically and economically thus have a strong incentive to use popular uprisings to their advantage, as defecting from the regime in favour of the opposition can enable the armed forces to outflank their competitors and obtain a privileged position in the post-regime political system" (Makara 2016, p. 215). Therefore, it can be assumed that the descended parts of the Libyan military had similar intentions, even though it seems that this did not find great resonance. Hence, the tool of technology networking and mobilization was quickly distorted through rebels seeking to establish a caliphate as it could be observed in the case of Daesh in the city of Sirte (at a time when the power vacuum spread rapidly and anarchic war scenarios were omnipresent).

> Libya's uprising was energised by the revolutions in Tunisia and Egypt, yet it followed a different path [...] (It) was both more violent and more prolonged, producing a situation described as 'civil war'. (Brahimi 2011, p. 606)

The Tribal Tradition in Libya: Questioning the Potential for Democracy

Undoubtedly, the tragic scenario in Libya in 2011 is due to Colonel Gadhafi's internecine violent actions against his own people, which inevitably led to the humanitarian intervention in March 2011. The situation on the ground shifted quickly and headed directly into chaos so that the momentum in which ICT could have been a beneficial tool was already lapsed.

Looking from a hypothetical perspective and assuming that the Libyan population could refer to equally advanced digital networking and mobilization as, e.g., the Tunisian or even Egyptian people, one must inevitably accept that the cyber-democracy phenomenon is merely a sufficient but not a necessary variable for democratic processing. Ultimately, it is first and foremost a tool, which renounces any positive or negative connotation.

It is thus the combination of the deeply rooted tribal culture that *seems* incompatible with the requirements of a modern democracy and the highly personalized policy that Gadhafi has pursued over four decades, thus creating a political tradition in which the people are immature and almost isolated from the outside world ("He

was never beholden to Western governments", Brahimi 2011, p. 610). *However, to postulate that such a tribal tradition is irreconcilable with modern democratic requirements, is simply too short-sighted and therefore must be rejected.* Furthermore, Robert F. Xavier and David F. J. Campbell elaborated that democracy and democratization can spread successfully to and can be successfully organized in Muslim-majority regions and countries (Xavier and Campbell 2014, p.167).

It is indeed remarkable that the "United Kingdoms of Libya adopted a federal system of governance, allowing considerable autonomy to each of its three provinces" (Brahimi 2011, p. 612). Therefore, on the contrary, it is more likely that this very effort of maintaining and protecting autonomous tribal cultures and traditions is a clear indication of Libyan self-determination. Accordingly, this should be taken into account, in such a way that should be integrated in the future democratic outcome of the Libyan state. For as Philip Howard correctly states:

> Quantitative researchers often turn democratization into an indicator for which the Western democracies are the standard [. . .] Democratization among these countries is best calibrated according to a more grounded standard, set at the high end by countries such as Turkey and Indonesia and at the low end by Libya and Turkmenistan [. . .] But it does assume that healthy functional Muslim democracies may not look like Western democracies. (Howard 2011, p. 27)

Initially, we have to understand that the so-called "state-building" process has never been a long-lasting success among nomadic people – with a view to the current situation in Northern Mali, where secession efforts and disputes are still on-going between nomadic tribes in the North and settled people in the South around the capital. This conflict in Mali turned out to be first and foremost a dispute about unequal distribution of resources that culminated in an ethnically charged one and therefore became even more political (Benetti 2008, p. 71). Consequently, it might be reasonably assumed that the situation in Northern Mali implies certain truths to Libya's current situation as well. In context, it could be that a greater part of the Libyan population is mostly concerned with a fair share of resources and economic profit opportunities, followed by adequate representation in the political outcome (since that might be already realized in their tribal worldview).

In essence, one could argue that, as already mentioned above, the tribal and nomad traditions in Libya are if anything contra-productive to state consolidation or even democracy-building. Evidently, there are several tribal families who are seeking adequate representation in the future state, as this is always the case when observing a country in transition and every group wants a share of power. It is thus hypothetically possible to develop a federal system where the main families and tribes are represented, integrated, and primarily in charge. In the same manner like South Africa, one could establish a federal state and each province is represented by the main tribe or main tribes. With regard to the sensitive and conflict-loaded question, what should be the capital city of Libya, one could propose to introduce a mode of a semiannual switching (for example, the first 6 months in Tripoli and the other 6 months in Benghazi). Also, the supervisory debate about the country's large oil resource must be given special consideration.

Libya's Oil Resources

"The holder of Africa's largest proved crude oil reserves" also harbors natural gas resources; in fact, Libya is the fifth-largest natural gas holder in Africa (US Energy Information Administration 2015, p. 1). The oil production is a nationalized enterprise named National Oil Corporation (NOC), which underlies the outdated petroleum law of 1955. Today, the World Bank estimates 39 billion barrels of crude oil resources and 51 billion cubic meters gas reserves, with a special view to the current status that three quarters of the country are still unexplored (Vrabl 2008, p. 117). Therefore, hopes are high that Libya bears even more undiscovered fossil reserves (Vrabl 2008, p.118). What sounds like a great blessing is at the same time Libya's weakest edge: A reduced dependency on the black gold is still not in sight, acknowledging that only 1% of the Libyan area is agriculturally viable, which proves the dependence on imported goods from abroad in reference to the most basic needs (75% of the food is still imported) (Vrabl 2008, p. 118). Concerning GNP (Gross National Product), only 3% of the Libyan population generates 60% of it. More than 50% of Libyans are working in the service sector; but this majority hardly obtains 9% of the GNP (the status as it was in 2005) (Vrabl 2008, p. 119).

> During the 2011 civil war, the drop in oil and natural gas production led to an economic collapse, and real gross domestic product (GDP) declined by 62% for the year. Libya's GDP growth rebounded in 2012, reflecting the relative stability of oil production, but it contracted by almost 14% in 2013 and by 24% in 2014, reflecting the ongoing production disruptions. (US Energy Information Administration 2015, p. 2)

The Libyan economy suffered a tremendous setback during the outbreak of the 2011's revolution, which created a stalemate in 2013 and 2014, when General Haftar returned to Libya after living in exile in the United States. "In addition, groups claiming to be affiliated with the Islamic State of Iraq and the Levant (ISIL) have severely damaged pipelines and vital equipment at oil fields in the eastern Sirte region that were operated by the Waha Oil Company, which includes companies from the United States, and an oil field operated by Total" (US Energy Information Administration 2015, p.5). "Before the 2011 war, Libya produced 1.6m barrels per day and accumulated more than $100bn in reserves" (Wintour 2017). Given the unmanageable chaotic and threatening situation, it is evident that no proper oil production can take place in current context.

> From January to October 2015, Libya's crude oil production averaged slightly more than 400,000 barrels per day (b/d), significantly below the 1.65 million b/d that Libya produced in 2010. (US Energy Information Administration 2015, p. 2)

Libya would do well in investing in more modern forms of the economy, but at this very moment, we cannot predict how the Libyan oil revenues will be managed in the near (or farther) future; however, this circumstance is tackled later on in a "thought experiment."

Algeria: A Lesson Learned?

To refer back to the real situation in Libya, it should be explored, how we can draw conclusions or even take lessons from former situations that may be comparable to Libya. In the case of Algeria, for example, a bloody civil war was breaking out in the 1990s, which lasted more than a decade, when an Islamist party was running the elections and was about to win. In 2005, Algerians agreed on a general amnesty (general pardon) to make an end to the killing and chaos. This act of forgiving is very controversial and reveals the stalemate of exhaustion the Algerian society found itself in. Certainly, this was additionally (perhaps) one of the many decisive reasons, why Algeria was not part of the Arab Spring. Like the North African neighbors, the Algerian society had and has sufficient reasons for criticizing their government, but the memory of the massacres (of the 1990s) was still too fresh to be unloaded in a (new) revolution.

> So, still scarred by the so-called Black Decade, Algeria did not witness a popular pro-democracy uprising in 2011, as happened in Tunisia and Egypt. (Ottaway 2012, p. 57)

Hence, the Libyan "civil war" (even though there are many voices who do not dare to speak of a civil war yet) might tend to have a likely cessation, bearing in mind that the armed conflict now enters its third year.

Scenarios: Different Experiments of Thought

The Fear of a New Somalia

> At the time of writing, Libya is in a process of Somalization. (Gaub 2013, p. 238)

To avoid the above-mentioned dread, it might be useful to recall and bear in mind that Libya, by now, may be heading toward chaotic conditions, observable likewise in Somalia. Considering the crucial amount of militias and rebel groups along with two to three rival governments that are fighting for and over influence and legitimacy, one could experience a future Libya that is being overshadowed with multiple de facto regimes with guerrilla characteristics. Somewhat cynically, this still might not happen due to the large oil resources Libya heritages:

> Diktator Gaddafi ist noch nicht endgültig besiegt, da konkurrieren Firmen um Libyens Erdöl. Den offiziellen Startschuss markiert die Wiederaufbaukonferenz in Paris. (Hassel 2011)

One could argue that it is indeed Libya's biggest fortune to be blessed with that kind of amount of fossil resources, since voices arose that the power and economic interests of the West was under the guise of the humanitarian intervention in 2011. Therefore, the natural resources have to be regarded as an asset and a potential

opportunity for supporting sustainable development, which should be targeted in the following scenario.

Investigating in Libya's Oil Policy

> In the long run, it does not appear to be realistic, to advance economy without also advancing democracy and democratization. (Xavier and Campbell 2014 p.166)

As Xavier and Campbell pointed out, there might be a link between economic prosperity and democratization processes in the long run. The bigger picture here is the following. We are in a position of expecting that a further diffusion of knowledge (knowledge, research, education, and innovation) should have at least in principle an effect in supporting and of further progressing processes of democratization. Knowledge society, knowledge economy, and knowledge democracy are in a process and development of interplay and mutual support, expressing core meanings of a "cyber-development" of a "cyber-democracy" (Campbell and Carayannis 2013, 2016a, 2016b; Carayannis and Campbell 2009, 2010, 2012, 2015). Of this one implication is: *Therefore, for Libya it will be crucial that the riches and revenues of natural resources will be transformed into sustainable development achievements for society within Libya.* Authors of an IMF Working Paper therefore recommend:

> Libya needs to establish an efficient and transparent PFM system, based on a medium-term fiscal framework with a consistent fiscal rule that reflects the country's economic objectives and the volatile nature of resource-based revenues. (Caceres et al. 2013, S. 25).

Among other mentioned economic models from different countries, the IMF Working Paper also refers to Norway on how these resources can be used in an effective way (also to master and to transform a switch from fossil energies to renewable energies):

> Norway uses a numerical fiscal rule that aims to keep the structural nonhydrocarbon budget deficit at 4 percent of the government's pension fund assets. This is an example of the conservative "bird-in-hand" strategy that explicitly excludes hydrocarbon revenues from the fiscal target, although there is room for temporary deviations over the business cycle. (Caceres et al. 2013, p. 25)

Cultivating a Strong Unified Military Force

It is more than obvious that rebuilding a state after an outburst of aggression and the emergence of revolutionary forces is a very challenging and often a long-lasting undertaking. One of the core tasks of state and sovereignty consolidation after a coup d'état are the disarming of militias and extremist groups and forming a consistent and uniformed military force:

> Rebuilding Libya's security forces will be a priority, both to demonstrate national independence from the North Atlantic Treaty Organization (NATO) and to act against any internal armed groups that choose violence over a peaceful political process. (Gill 2011)

Even though westernized minds could be alerted when thinking of a new Libyan military force with regard to the circumstance that the notorious General Haftar seeks to be the sole commander of the future Libyan military, the recultivation is still more than essential to the future Libyan state. Since the Libyan population urges to establish stability and security in their everyday lives, this should be one of the main responsibilities of the military forces. Critical voices worrying about a next military dictatorship in the MENA (Middle East and North Africa) region, under the command of General Haftar, have to recognize the great urgency to install a respectful counteragent to the present power vacuum, especially with regard to the lack of diplomatic relationships with the rest of the world. Nevertheless, the geopolitical position of Libya bears great dangers, referring to the refugee situation, which goes beyond the Libyan border and thus affecting numerous countries, not to mention the direct border situation with Tunisia or Egypt, where the populations may fear spill-over effects from and through Libya due to the greatly abandoned weapon arsenal of the Libyan military in 2011 (as it was the case when Libyan Tuareg fighters joined the Azawad movement in Northern Mali, well equipped with Libyan weaponry in 2011). Subsequently, reforming a strong military force unit, maybe with the supervision of a new international UN mandatory, is also in the very interest of European or Western democracies.

Conclusion

From the countries of the Arab Spring, so far, only Tunisia has managed to follow successfully a path toward more democracy and democratization. By this, Tunisia represents potentially a "role model" for a transformation from authoritarianism toward democracy (more democracy) for the whole (MENA) region of the Arab (post-Arab-Spring) countries. A vast majority of the other Arab countries clearly suffered from a decline in levels of democracy or modest democracy, when the years 2011–2012 and 2014–2015 are taken as reference points (concerning the Democracy Ranking 2016, see for more details in Campbell et al. (2017)). While Tunisia increased with emphasis its scoring on quality of democracy in a positive sense (see Table 1), the other Arab countries (for example, Egypt, Syria, but also Libya) suffered from a further decline in levels of democracy and democratization (on methodic options for a systematic democracy measurement see: Campbell et al. 2013).

From the very beginning, Libya's dilemma was interwoven with international Western conditions. Since the turmoil in 2011, the situation now has become highly diffused and unclear regarding the multiple rival groups and the (two or more) competing governments, so that a fast and efficient solution is still not in close sight. Although the media coverage hardly reports on the current situation, with the

Table 1 The development of quality of democracy in core countries of the Arab Spring (years 2011–2012 and 2014–2015 in comparison). Countries ranked according to scores, Norway serves as a reference country (reference democracy)

	Years 2011–2012	Years 2014–2015	Changes in scores
Norway	99.6	100.0	+0.4
Tunisia	37.1	48.6	+11.5
Egypt, Arab Republic	19.8	15.4	−4.4
Libya	14.8	6.7	−8.1
Syrian Arab Republic	4.3	0.0	−4.3

Methodic note: Scoring spectrum extends from 0 (the lowest observed democracy value) to 100 (the highest observed democracy value)
The Democracy Ranking 2016 samples and compares 113 countries, and there ranks Norway (2014–2015) the highest and Syria (2014–2015) the lowest
Source: Authors' own calculations based on the Democracy Ranking 2016 (Campbell et al. 2017)

major exceptions of the "refugee crisis" or security issues, one could get the impression that this symbolizes somewhat a growing reconciliation and inner stability, when there is nothing to report about. Yet, the opposite is the case: the government around Prime Minister Fayez al-Sarraj is being regarded by its opponents as a puppet of the West, which strains the establishment of loyalty and support in the Libyan population, complicating the prospects for the internationally created Libyan Political Agreement (LPA) that was set up in December 2015. Currently, the Libyan Government of National Accord (GNA) still is not being accepted and supported by all political parties and fractions in Libya, and there is operating a government conflict and a government competition between Tripoli and Tobruk, creating a "Tripoli government" and a "Tobruk government". To this day, the Tobruk-based House of Representatives (HoR) does not (sufficiently) support the Government of National Accord (GNA), which is based in Tripoli. Hence, it is crucial that the Libyan self-determination finally finds its voice and that the West has to concede that the rushed humanitarian intervention in 2011 was also interconnected to several troublesome effects afterward. Libya should not become a battlefield of rivalling Western power interests. Plus, it is of particular importance that the United Nations appoints a new UN Libyan special envoy.

> Toaldo has said that the diplomatic vacuum has been made worse by the effective end of the role of Martin Kobler, the UN Libyan special envoy. (Wintour 2017)

As it was suggested to include the tribal traditions in the new political outcome, "Kobler announced his intention to work on the creation of a Grand Shura Council, which would include mayors and tribal leaders. [...]This General Assembly should be a political forum for national dialogue and reconciliation, not a legislative authority to rival the House of Representatives or the State Council" (ecfr.eu)

> A broad framework for decentralisation at city council level could bring together all parts of Libya. This would go some way towards appeasing the unity government's opponents who are currently gathered around General Haftar (Toaldo 2016, p. 9)

Moreover, it is not only about combatting extremist ISIS and other terrorist groups – crucial challenges are, as it was mentioned in the previous sections of this analysis – to invest in developing a new (and responsible) military leadership and to establish a functioning economy. Obviously, this target will be very laborious and protracted, reflecting that the Libyan misère is a very exceptional and unprecedented case. Nevertheless, the construction sites of Libya and Libyan society are well known, which is at least something positive.

In conclusion of our analysis, we again want to propose the following discussion points as possible references for a thinkable master plan toward more democracy and democratization in a future Libya (on quality of democracy in global context, see also the discussion in: Campbell et al. 2015; Carayannis and Campbell 2014):

1. *Lessons to be learned (by Libya) from positive examples of democratization in Arab countries (MENA region), lessons to be learned for others from Libya:* In a majority of the cases, the developments in the aftermath of the Arab Spring have not lead to more democratization in the Arab countries. However, the one positive example here is being represented by Tunisia, because Tunisia realized an increase in democracy and quality of democracy in recent years. Therefore, the developments in the potential role model of Tunisia should be analyzed very carefully, so to contribute in helping to assess, what Libya could possibly learn from Tunisia. However, also the other Arab countries should inquire what they may want to learn from Libya and possible reforms in Libya.
2. *Further federalization, perhaps con-federalization of the state of Libya:* Allowing for a greater regional autonomy within Libya may define and represent one strategy, how to balance the different regional (and ethnical) interests. This also could be regarded as a step forward toward federalizing or even con-federalizing Libya. The parliament could be designed as a bicameral system, balancing national representation with different, diversified, and specific regional representation (currently, the legislature of Libya is only unicameral). The status as a capital city of Libya can rotate (switch) between Tripoli and Benghazi on a regular and continuously permanent basis (to formulate an example). Libya should also reflect how to translate the (close) neighborhood to the European Union (in its North) into an advantage and asset for Libya.
3. *The use of the natural resources of Libya for a Broader and Greater Policy Plan in the directions of a sustainable development: Libya should leverage on the richness of its natural resources (most prominently, the fossil energies), so to transform those revenues into purposes of a sustainable development*. For that, specific and focused policy measures must be designed and applied. *The goal of sustainable development would refer to be building a knowledge society, knowledge economy, and knowledge democracy: and fossil energies should add in financing (cofinancing) such a mid-term and long-term path of development*. Here cyber-democracy and cyber-development would come together, in theory and practice. *In a smart strategy format, economic opportunities and reflected political state-building can further finally democracy-building in Libya and in a Libya of tomorrow.*

References

Al-Afifi, F. (2012). War of creative destruction: The central tendency in the globalized Arab revolutions (a study in the formation of the future). *Contemporary Arab Affairs, 5*(3), 427–447.

Benetti, T. (2008). Entwicklung des Verhältnisses zwischen Tuareg und staatlichen Strukturen in Mali. Wien: o.V., Accessed 16 Apr 2017. http://othes.univie.ac.at/2030/1/2008-11-02_9807842.pdf.

Brahimi, A. (2011). Libya's revolution. *The Journal of North African Studies, 16*(4), 605–624.

Caceres, C., et al. (2013). The day after tomorrow: Designing an optimal fiscal strategy for Libya. *International Monetary Fund, 2013*(79.) Accessed Apr 16 2017. http://www.elibrary.imf.org/view/IMF001/20381-9781484389812/20381-9781484389812/20381-9781484389812.xml.

Campbell, D. F. J., & Carayannis, E. G. (2013). Epistemic governance in higher education. In *Quality enhancement of universities for development*, *SpringerBriefs in Business*. New York: Springer. http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6.

Campbell, D. F. J., Carayannis, E. G., Barth, T. D., & Campbell, G. S. (2013). Measuring democracy and the quality of democracy in a world-wide approach: Models and indices of democracy and the new findings of the "democracy ranking". *International Journal of Social Ecology and Sustainable Development, 4*(1), 1–16. http://www.igi-global.com/article/measuring-democracy-quality-democracy-world/77344.

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493. http://link.springer.com/article/10.1007/s13132-015-0246-7.

Campbell, D. F. J., & Carayannis, E. G. (2016a). Epistemic governance and epistemic innovation policy. *Technology, Innovation and Education, 2*(2), 1–15. https://doi.org/10.1186/s40660-016-0008-2. http://technology-innovation-education.springeropen.com/articles/10.1186/s40660-016-0008-2.

Campbell, D. F. J., & Carayannis, E. G. (2016b). The academic firm: A new design and redesign proposition for entrepreneurship in innovation-driven knowledge economy. *Journal of Innovation and Entrepreneurship, 5*(12), 1–10. https://doi.org/10.1186/s13731-016-0040-1. http://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-016-0040-1.

Campbell, D. F. J., Pölzlbauer, P., & Barth, T. D. (2017). *Democracy ranking 2016*. Vienna: Democracy Ranking Organization. http://democracyranking.org/wordpress/.

Carayannis, E. G., & Campbell, D. F. J. (2009). "mode 3" and "quadruple helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46*(3/4), 201–234. http://www.inderscience.com/browse/index.php?journalID=27&year=2009&vol=46&issue=3/4 and http://www.inderscience.com/search/index.php?action=record&rec_id=23374&prevQuery=&ps=10&m=or.

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69. http://www.igi-global.com/bookstore/article.aspx?titleid=41959.

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development*, *SpringerBriefs in Business*. New York: Springer. http://www.springer.com/business+%26+management/book/978-1-4614-2061-3 and http://www.springer.com/cda/content/document/cda_downloaddocument/9781461420613-c1.pdf?SGWID=0-0-45-1263639-p174250662.

Carayannis, E. G., & Campbell, D. F. J. (2014). Developed democracies versus emerging autocracies: Arts, democracy, and innovation in quadruple helix innovation systems. *Journal of Innovation and Entrepreneurship, 3*, 12. http://www.innovation-entrepreneurship.com/content/3/1/12.

Carayannis, E. G., & Campbell, D. F. J. (2015). Art and artistic research in quadruple and quintuple helix innovation systems. In G. Bast, E. G. Carayannis, & D. F. J. Campbell (Eds.), *Arts, research, innovation and society* (pp. 29–51). New York: Springer. http://link.springer.com/chapter/10.1007/978-3-319-09909-5_3.

Djaziri, M. (2009). Tribus et Ètat dans le Système Politique Libyen. *Outre-Terre, 3*(29), 127–134.

El-Nawawy, M., & Khamis, S. (2012). Cyberactivists paving the way for the Arab spring: Voices from Egypt, Tunisia and Libya. *Cyber Orient – Online Journal of the virtual Middle East, 6*(2). Accessed Apr 16 2017. http://www.cyberorient.net/article.do?articleId=7994.

Erdmann, G. (2002). Neopatrimoniale Herrschaft - oder: Warum es in Afrika so viele Hybridregime gibt. In P. Bendel (Ed.), Zwischen Demokratie und Diktatur (pp. 323–342). Wiesbaden: Verlag für Sozialwissenschaften.

Erdmann, G. (2014). Apocalyptic triad: State failure, state disintegration and state collapse: Structural problems of democracy in Africa. *Zeitschrift für Vergleichende Politikwissenschaft. Comparative Governance and Politics. Wiesbaden: Springer Fachmedien, 8*(3), 215–236.

Gaub, F. (2013). The Libyan armed forces between coup-proofing and repression. *Journal of Strategic Studies, 36*(2), 221–244.

Gill, B. (2011, May 26). Libya at the crossroads – the challenge of consolidating peace. Accessed 16 Apr 2016. https://www.sipri.org/commentary/essay/thu-05-26-2011-14-00/libya-at-crossroads-challenge-of-consolidating-peace.

Haimzadeh, P. (2015, April 9). Libyen – der zweite Bürgerkrieg. *le monde diplomatique*. Accessed Apr 16 2017. http://monde-diplomatique.de/artikel/!200131.

Hassel, F. (2011, September 01). Der Kampf um die größten Ölvorräte Afrikas beginnt. *welt.de*. Accessed Apr 16 2017. https://www.welt.de/wirtschaft/article13578982/Der-Kampf-um-die-groessten-Oelvorraete-Afrikas-beginnt.html.

Howard, P. N. (2011). *The digital origins of dictatorship and democracy: Information technology and political Islam*. Oxford: Oxford University Press.

Kranzberg, M. (1986). First law of technology. *Technology and Culture, 27*(3), 544–560.

Makara, M. (2016). Rethinking military behavior during the Arab spring. *Defense & Security Analysis, 32*(3), 209–223.

Turnhout, E. (2010). Heads in the clouds: Knowledge democracy as a utopian dream. In R. J. in't Veld (Ed.), *Knowledge democracy* (pp. 25–36). Berlin: Springer.

Omar, M. (2012). Libya: Rebuilding from scratch. In R. Wright (Ed.), *The Islamists are coming: Who the really are* (pp. 49–56). Washington, DC: Woodrow Wilson Center Press.

Ottaway, D. B. (2012). Algeria – Bloody past and fractious factions. In R. Wright (Ed.), *The Islamists are coming: Who the really are* (pp. 57–71). Washington, DC: Woodrow Wilson Center Press.

Schwarz, R. (2012). Libyen und das dilemma externer Interventionen. *Der Bürger im Staat, 62*(1/2), 34–43.

Toaldo, M. (2016 May). Intervening better: Europe's second chance in Libya. European Council on Foreign Affairs website. Accessed Apr 16 2017. http://www.ecfr.eu/page/-/ECFR172_-_INTERVENING_BETTER_-_EUROPES_SECOND_CHANCE_IN_LIBYA_2.pdf.

U.S. Energy Information Administration. (2015, November 19). Country Analysis Brief: Libya. eia website. Accessed Apr 16 2017. https://www.eia.gov/beta/international/analysis_includes/countries_long/Libya/libya.pdf.

Vrabl, A. (2008 July). Libyen: Eine Dritte Welt – Revolution in der Transition. Diploma thesis. University of Vienna, Wien.

Wintour, P. (2017, March 29). Struggle for control of Libya's oil threatens to deepen conflicts. *The Guardian*. Accessed Apr 16 2017. https://www.theguardian.com/world/2017/mar/29/struggle-for-control-of-libyas-oil-threatens-to-deepen-conflicts.

Xavier, R. F., & Campbell, D. F. J. (2014). The effects of Cyberdemocracy on the Middle East: Egypt and Iran. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 147–173). New York: Springer. http://link.springer.com/chapter/10.1007/978-1-4939-1028-1_5.

The Political Economy of Drone Warfare

15

Hamid R. Ekbia

Contents

Abstract

The expanding use of armed drones as weapons of war has put them squarely at the center of military strategy by a growing number of countries. The appeal of drones to military strategists derives from their greater scope and range of operation, endurance, and alleged precision. What makes this sudden expansion especially curious, however, is that drone technology has been around for quite a

H. R. Ekbia (✉)
School of Informatics and Computing, School of Global and International Studies, Indiana University, Bloomington, Bloomington, IN, USA
e-mail: hekbia@indiana.edu

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_40

long time. Beyond technical and military capabilities, therefore, one needs to examine the broader socioeconomic, geopolitical, and cultural transformations that have pushed drones to the center stage on a global scale. In particular, epochal changes in the governance of capitalist economies provide the main backdrop for these developments. This chapter examines drone technologies and drone warfare as a point of convergence among three key developments: (i) the emergence of a new spirit of capitalism and, along with that, a new globalized economy defined by hyperconnectivity, hyperspeed, and polarization; (ii) the decline of nation-states as the dominant model of territorial governance and the rise of the model of government at a distance in developed liberal economies, on the one hand, and of non-state, informal, and illicit actors and organizations in a large part of the globe, on the other; and (iii) the development of a "new war" that borrows elements from earlier revolutionary, counterinsurgency, and "just" wars of the past. This chapter also examines some of the psychological, social, and global implications of drone warfare for individuals, communities, and societies around the globe, tracing the presence of computing technologies and practices throughout.

Keywords
Capitalism · Computing · Globalization · Terrorism · Polarization · New war

Introduction

The use of armed drones has, for the last few years, expanded in military operations by a select number of countries, especially the USA and Israel. The expanding use of these technologies as weapons of war has put them squarely at the center of military strategy, policing, and the so-called war on terror in the USA and beyond, with a growing number of countries around the globe seeking to develop or purchase drones for foreign and domestic operations. According to reports, more than 70 countries around the globe have currently developed some kind of drone capacity.

The appeal of drones to military strategists derives from their greater scope, range, and endurance, as well as their alleged precision. For the first time in the history of war, drones allow the location of their operators to be determined solely based on safety, security, and convenience. Mindful of this unique feature set, the military has used drones to perform 3D ("dull, dirty, and dangerous") missions – e.g. long-haul flights, reconnaissance operations that require hours and hours of hovering over an area, or combat situations that incur high risk to pilot life. In sum, the idea is that by combining remote fight and remote flight, one can "find, fix, and finish" enemy combatants with surgical precision and cleanness – that is, with little or no collateral damage or civilian casualty.

In 2003, when the USA invaded Iraq, only a few drones flew over the region, mostly in support roles for the ground troops. Today, the US military has procured and operates thousands of drones ranging in size from very tiny to small airliners,

along with dozens of Predators and Reapers that fly over Africa, the Middle East, and Central Asia round the clock, 24 h a day, 7 days a week. Accordingly, the total number of flight hours by drones went through a tenfold increase in the 10 years between 1999 and 2009, from almost 20,000 h to 200,000 h, and it has continued to increase with a faster pace since then. In particular, the focus on drones as a key component of counterinsurgency operations by the Obama Administration marks a strategic shift, which was put into high relief by the appointment in 2015 of Ashton Carter, the former head of drone acquisitions at the Department of Defense, as the Secretary of Defense.

What makes this strategic shift especially curious is that drone technology has been around for quite a long time. The history of drones goes back to the end of the nineteenth and beginning of the twentieth century, when the very first unmanned airplanes were used as decoys for aerial combat. On May 6, 1896, Samuel Langley, secretary of the Smithsonian, launched a steam-powered drone dubbed the *Aerodrome* over the Potomac River near Washington, D.C. In WWI, drones were used as decoys; and in WWII for training of antiaircraft personnel. Their use was extended to reconnaissance during the Cold War and to intelligence and surveillance during the Gulf War. It is only in the last few years that drones such as the Predator have become weapons of war on a global scale, giving rise to numerous questions about technical and military capabilities of drone technology, the legality and morality of drone warfare, and its short- and long-term social, cultural, and geopolitical implications.

These are all significant questions, which have received broad commentary from military, legal, and security experts, political pundits, moral philosophers, and others. A key question that has remained largely unaddressed is a historical one: *Why now?* What parameters have pushed drones to the center of military strategy at this moment in history? This is the central question of the present analysis, the answer to which should be found beyond the technical capabilities of modern drones and the military advantages that they provide. The answer should also go beyond "identity politics," which seeks to understand modern warfare in terms of national, ethnic, and religious identities and agendas of warring parties – a view that finds strong advocates across the political spectrum, particularly on the right. The answer, rather, can be more meaningfully explored within the broader context of socioeconomic, political, and global developments of recent years. The technical and military discourse of drones as advanced aviation vehicles, equipped with sophisticated visual and surveillance technology, and armed with "smart weapons" of high precision, can be understood in light of the socioeconomic, geopolitical, and institutional considerations that provide it with meaning. In particular, the discourse derives meaning from a set of intersecting developments: (i) the socioeconomic displacements of new capitalism; (ii) the changing character of politics, governance, and nation-states; and (iii) the institutional transformation of war and militaries – in brief, a new economy, a new politics, and a new model of war. In what follows, I briefly describe these developments and illustrate how they have come to converge, at the present moment, on drone warfare. Computer technology, as we shall see, is a key component of all of these developments, although it does not necessarily drive them.

New Economy: Hypercapitalism

During the last century or so, the spirit of capitalism has drastically changed. By "spirit of capitalism," I mean the underlying principles that dictate the logic of action for societies, institutions, and individuals. At the core of these principles is Benjamin Franklin's dictum that "money begets money and . . ." The sociologist Max Weber famously described this dictum as a "philosophy of avarice," which sees the accumulation of money (or, more accurately, capital) as an end in itself. Since the philosophy of avarice is deeply irrational – why should one pursue capital accumulation beyond individual utility and consumption? – it needs to be justified through mechanisms of consent making and enforced through mechanisms of social control.

The spirit of capitalism, therefore, consists of the principle of permanent accumulation, along with a way of life that is promoted through the mechanisms of justification, consent, and control. It is this spirit that has changed dramatically, and more than once, since the times of Weber. While the underlying principle of accumulation has remained constant, all the other components have functioned as moving parts that are adjusted in order to guarantee capital growth. To maintain growth, capitalist economies have to devise new ways of creating value – they have to *innovate*. Innovation is often associated with technology, but it also has to happen with respect to the mechanisms of control and consent.

In the last three decades, largely thanks to the implementation of neoliberal policies, capitalism has attained a new spirit (Boltanski and Chiapelo 2005). In particular, the intensive computerization and connectivity of the economy through broad dissemination of the internet around the globe has given rise to a capitalism that can perhaps be described as "hypercapitalism." The key attributes of hypercapitalism are hyperconnectivity, customization, and hyperpolarization.

Hyperconnectivity

The economy of the globe has been connected for many centuries through trade, financial transfers, credit systems, etc. (Braudel 1977). Globalization in this basic sense is, therefore, not new. What is novel is the intensity of connections among local and national economies, which has in turn intensified the flow of commodities, labor, and capital around the globe. Kaldor (2006) describes the key features of this new economy in terms of decline in the importance of territorially based production, globalization of finance and technology, and increased specialization and diversity of markets. Some of the implications of these features are the decline of the working class, income disparity, and the globalization of inequality (Bourguignon 2015), which provides the economic backdrop for the growth of migration, terrorism, and drone warfare.

Hyperconnectivity has also enabled the speeding up of economic processes in almost all areas, from production and manufacturing to trading, distribution, and consumption. Concepts such as just-in-time delivery, fast trading, and customized consumption are emblematic of this phenomenon, as is "customization" of products and services.

Customization

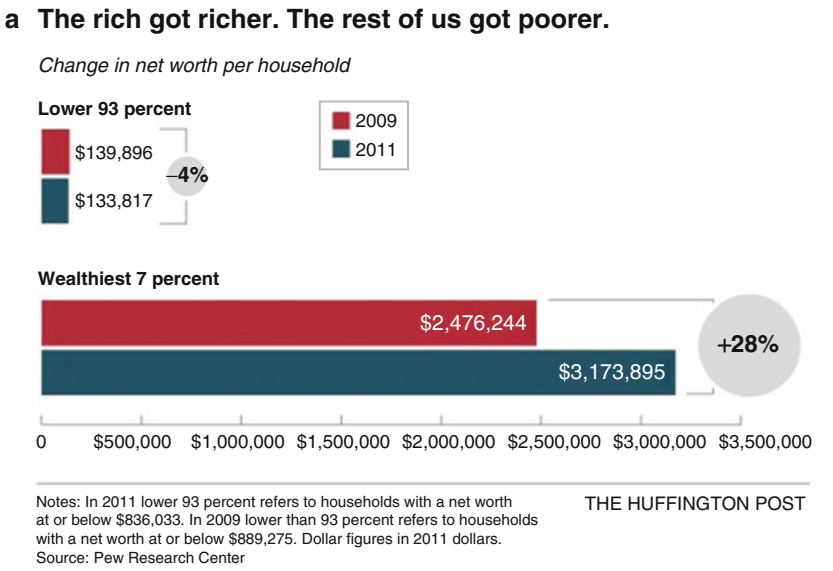
Customization often takes the form of personalized interfaces that adapt themselves to the demands, tastes, and whims of the user, often according to the template that comes in the form of "My X" – "My Yahoo," "My Newsfeed," "My Favorites," and so forth. Web 2.0 took this idea further from form and interface to customized content, where users receive all manner of cultural, political, and consumer products in the shape of RSS news feeds and recommendations (e.g., books and other products on Amazon, music on Pandora, movies on Netflix). These customizations are increasingly performed by actors unknown to the average user, using big data techniques of machine learning and data analytics, and giving rise to concerns about privacy, surveillance, etc. The implications are much broader, however, in terms of social equity and the distribution of wealth – e.g., in terms of disparity in access to resources such as "cloud" infrastructures that give major corporations monopolistic control (Ekbia et al. 2015). The same techniques of "customization," as we shall see, are also applied to drone warfare, where war is waged by governments against individually identified insurgents.

Polarization

The net effect of hyperconnectivity, hyperspeed, and customization is the high degree of polarization in terms of the distribution of income, wealth, consumption, etc. This is evident in diverging trends between corporate profits and stock indices in the years after the Great Recession, on the one hand, and, on the other, the much slower growth in earned wages during the same period. Rising stocks and profits have widened the income gap between the top 7% and the rest of the population (Fig. 1a). According to the economist Emmanuel Saez, the share of the wealthiest Americans of the national income is higher now than at any point since before the Great Depression. A key difference, however, is that, unlike the Depression, current policies are typically not aimed at equality (Gongloff et al. 2013). Instead, based on what Joseph Stiglitz describes as a nefarious combination of ideology and interest, "inequality-enhancing policies. . .[design] the rules of the game to ensure this outcome" – namely, political and economic inequality (2014).

The decline in income of a large segment of the population means a reduction of tax revenues for the government. In the USA, for example, tax revenues declined from $2.5 trillion in 2008 to $2.1 trillion in 2009 and remained at that level in 2010. During the same period, individual income taxes declined 20%. The drop in tax income was further exacerbated by tax policies that favor corporate business. Corporate taxes declined 50% from 2008 to 2009. At 14.6% of GDP, the 2009 and 2010 collections were the lowest level of the past 50 years, raising the federal debt in the foreseeable future (Congressional Budget Office 2015; see Fig. 1b).

The reduction in tax revenue explains the austerity policies advocated by conservative economists and politicians, but it also explains the impetus for harnessing military spending. The growing trend of military spending during George W. Bush administration was simply not sustainable. According to the Congressional Budget



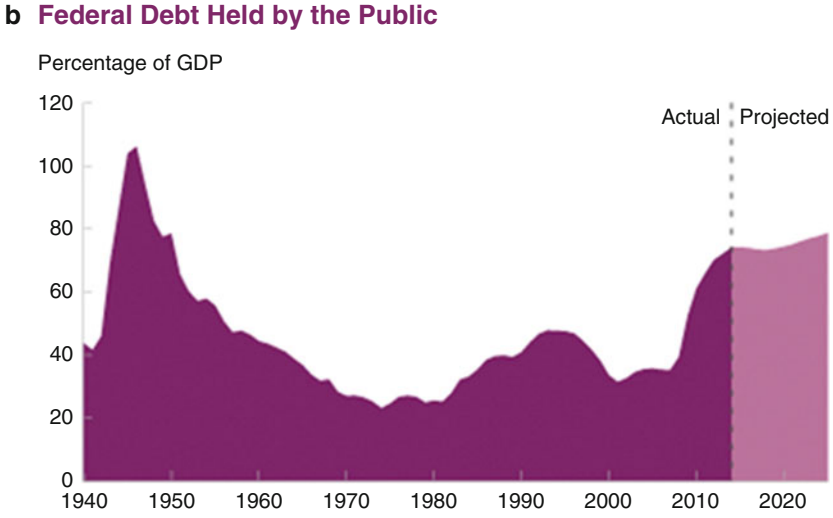


Fig. 1 (**a**) The recovery pattern in the USA after the *Great Recession of 2008;* (**b**) Changes in federal debt in the USA

Office, defense spending in the USA grew from $297 billion in 2001 to a budgeted $534 billion for 2010, an overall increase of 81%. In 2010, the defense budget accounted for about 19% of the US federal budgeted expenditures and 28% of estimated tax revenues. Including non-DOD expenditures, military spending was approximately 28–38% of budgeted expenditures, 42–57% of estimated tax revenues, and around 4% of GDP.

This trend peaked in 2013, when the military budget (including the Department of Defense, the Department of Veterans Affairs, and the Department of Homeland Security) surpassed $800 billion. It was only in 2014 that a reversal was noticed, with the budget falling to approximately $33 billion or 4.1% below 2013 spending. DOD spending had already fallen from a peak of $678 billion in 2011 (Fig. 2).

The push toward drone operations can be partly understood in terms of these financial figures. A close look at the components of reduction in military spending shows the key areas of saving (see Table 1). As seen in the table, the key areas of significant saving are in operations, maintenance, and military personnel – areas where drones can be claimed or perceived to be most effective.

New Politics: Action at a Distance

The broad economic trends outlined above have their surrogates in the political sphere at both domestic and global scales. Three key transformations are perhaps most relevant to the expansion of drone warfare: (i) the new model of *government at a distance* in developed countries, (ii) the collapse or disintegration of nation-states in many parts of the developing world, and, as a result of these, (iii) the disengagement of the public from the war effort in the developed world, on the one hand, and the escalating impact of war on civilian populations in the developing world. We briefly examine these transformations here.

Government at a Distance

The reversals in capitalist economies launched in the 1980s provided the beginnings of a process of the unraveling of the welfare state in the West. In the USA, in particular, these policies took away many of the benefits and protections available to the population after WWII through the implementation of the New Deal by the Roosevelt Administration. Neoconservative policies followed by George W. Bush took these measures to a whole new level, seeking to privatize all types of social support systems. The model of government that was to be implemented through these policies can be described as "government at a distance." This is a kind of government that operates within an environment of deregulation, privatization, and minimal intervention on the part of the state (Miller and Rose 2013).

In light of these trends, governance has also become regionalized and transnational. This has, in turn, increased the importance of transnational organizations and treaties, as well as nongovernmental actors and networks.

The Weakening of Nation-States

The same policies that gave rise to the new model of government in the developed world had different effects on the opposite side of the globe, where the collapse of

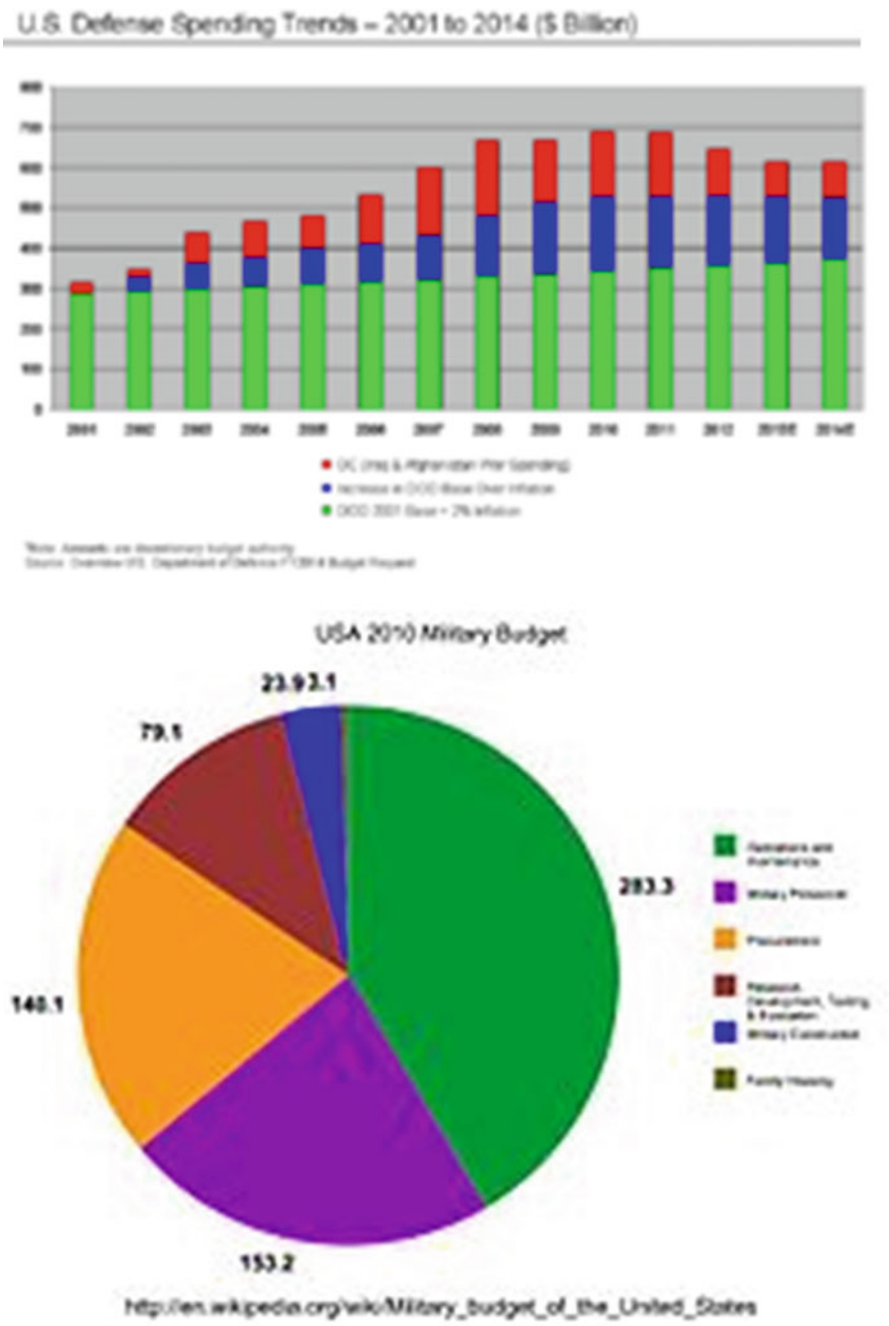


Fig. 2 Trends in military spending in the USA

Table 1 Key areas of military spending in the USA

Components	Funding (billion)	Change, 2012–2013 (%)
Operations and maintenance	$258.277	−9.9
Military personnel	$153.531	−3.0
Procurement	$97.757	−17.4
Research, development, testing & evaluation	$63.347	−12.1
Military construction	$8.069	−29.0
Family housing	$1.483	−12.2
Other miscellaneous costs	$2.775	−59.5
Atomic energy defense activities	$17.424	−4.8
Defense-related activities	$7.433	−3.8
Total spending	**$610.096**	**−10.5**

the Soviet Union deprived many governments of a major source of economic, political, and military support.

The conditions dictated by global financial institutions such as the World Bank or the International Monetary Fund exacerbated this situation by imposing neoliberal policies that ruined local economies, pushing large segments of the population toward unemployment, poverty, conflict, and migration. As a result, many of these governments were deprived of a reliable tax base, unable as they were to provide their population with basic security and social services, or to devise and implement successful economic policies of welfare. They were simply too weak to govern effectively:

> A downward spiral of loss of revenue and legitimacy, growing disorder, and military fragmentation creates the context in which the new wars take place. Effectively, the 'failure' of the state is accompanied by a growing privatization of violence. (Kaldor 2006, 97)

The void created by this was filled by religious ideologues and organizations, tribal militias, autocratic rulers, or a combination of these, depending on local histories and specific circumstances. Unlike the developed world, where privatization was implemented in a legal environment that favored corporate-friendly regulations, here privatization emerged in an environment of lawlessness, propelling small and large militias, warlords, and clandestine organization to the center stage of world politics. These entities finance their wars through illicit methods such as looting, robbery, extortion, and hostage taking, as well as the imposition of war taxes and "protection." As Kaldor (2006) points out, "essentially, the fragmentation and informalization of war is paralleled by the informalization of the economy" (p. 110).

The Public: At Risk but Disengaged

The overall effect of this kind of governance is "the insecurity of the contemporary situation, both physical and material" (Kaldor, p. 162). Although the

current situation is economically similar to the period before WWII, there are significant political differences that make the two situations dissimilar. In WWII, everyone was mobilized for the war effort, largely because the political mood was one of engagement and participation. In the current situation and in the shadows of the long-stretched wars in Vietnam, Iraq, and Afghanistan, the majority of the US population is socially and politically isolated (Kaldor 2006, p. 168).

The American journalist and writer James Fallows (2015) describes the current situation in terms of public engagement with war in the USA as follows:

> Americans admire the military as they do no other institution. Through the past two decades, respect for the courts, the schools, the press, Congress, organized religion, Big Business, and virtually every other institution in modern life has plummeted. The one exception is the military. Confidence in the military shot up after 9/11 and has stayed very high. In a Gallup poll last summer, three-quarters of the public expressed "a great deal" or "quite a lot" of confidence in the military. . . ..
>
> Too much complacency regarding our military, and too weak a tragic imagination about the consequences if the next engagement goes wrong, have been part of Americans' willingness to wade into conflict after conflict, blithely assuming we would win.

This "willed amnesia," as Fallows describe it, finds an effective vehicle of implementation in drones. Based on what the French philosopher Chamayou (2015) describes as "necroethics," drones provide the possibility of nonreciprocal combat, where you can kill without putting yourself at the risk of being killed.

The asymmetry of drone warfare affects people's daily life in targeted areas in a totally different way. Beyond injury and death, here people have to constantly face the fear and anxiety of a deadly attack. This constant fear gives rise to what psychologists call anticipatory anxiety, which has short- and long-term implications for daily life as well as for communal and cultural life. A joint study by Stanford and NY Universities of Waziristan Province in Pakistan identified the impacts of drone strikes on these communities, including the following:

- Unwillingness to rescue victims and provide medical assistance
- Property damage and economic hardship
- Loss of education opportunities because people are reluctant to send their children to school in fear of drone attacks
- Weakening of local traditions such as funerals, weddings, etc.
- Increased mistrust in the community

This is what one villager told the study team:

> We are always thinking that it is either going to attack our homes or whatever we do. It's going to strike us; it's going to attack us . . .. No matter what we are doing, that fear is always inculcated in us. Because whether we are driving a car, or we are working on a farm, or we are sitting home playing . . . cards – no matter what we are doing, we are always thinking the drone will strike us. So we are scared to do anything, no matter what. (International Human Rights 2012)

New Wars: Hybrid Networks of Humans and Machines

If war, as famously formulated by Clausewitz, is "the continuation of politics by other means," then how has the changing mode of governance affected modes of combat and the character of war? If new governance is defined by action at a distance, what defines the character of new wars? Mary Kaldor describes new wars as ones "fought by loose networks of state and non-state actors" (158). On close examination, these networks are hybrid arrangements of humans and machines.

Human Networks: Targeted Killing

Drone strikes by the USA are performed by both military and nonmilitary agencies such as the US Air Force, the Army, the CIA, and perhaps others. Although there is no publicly known division of labor among these agencies, to best of our knowledge they pursue different types of targets, using different types of techniques. Two officially recognized types of strikes are called "targeted killing" and "signature strikes." Targeted killings refer to the assassination of prespecified individuals on the basis of their (perceived) role in an insurgent organization, or what is technically referred to as a "disposition matrix." The elimination of terrorist leaders through this technique has certainly disrupted the plots and operations of Al-Qaeda, but the vast majority of reported drone strikes do not kill high-value targets or, indeed, any member of a terrorist organization.

According to reports by the Bureau of Investigative Journalism, of the 2,500–3,500 estimated deaths from drones in Pakistan, only 70 individuals – around 2.3% – were ranking members of Al-Qaeda. The remainder were mid-to-low-level commanders and fighters, and around 474–881 civilians, including 176 children. American and European citizens and aid workers have also been victims of such attacks – a reported example being Warren Weinstein and Giovanni Lo Porto, two American and Italian aid workers who were captured by Al-Qaeda in Afghanistan and held for ransom in Pakistan's Shawal Valley, until they were killed by US drone attacks in early 2015.

Machine Networks: Signature Strikes

The second type of drone strike is called signature strike, which is based on "pattern of life" analysis. According to US authorities, these strikes target "groups of men who bear certain signatures, or defining characteristics associated with terrorist activity, but whose identities aren't known." Just what those "defining characteristics" are has never been made public, but the technique used for this kind of analysis are based on big data methods that collect, compile, and analyze data from various sources for the purpose of predictive modeling. In this case, the data collected about individuals can come from their social networks, locations, phone contacts, or basic demographic information such as age, ethnicity, tribal affiliation, and so forth.

Hybrid Networks

Targeted killings and signature strikes take the logic of "new war" to its ultimate limit. New warfare, according to Kaldor (2006), borrows elements from both revolutionary wars of the past and counterinsurgency operations of modern states. Rather than capturing territory, the aim of new wars is to control territory through political means, and rather than popular support, they seek to accomplish their objectives through population displacement by creating an unfavorable environment for populations that cannot be controlled (Kaldor 2006). Drone warfare, we might add, pursues these objectives selectively, making the environment unfavorable for insurgents and those members of the population that are disposed to act in certain ways.

It is in this spirit that the techniques of big data, computer modeling, and social analysis are combined with traditional techniques of surveillance, intelligence gathering, and espionage in hybrid networks humans and machines.

Impacts of Drone Warfare

Military drones, as we see, are not simply sophisticated technologies; they are the point of convergence of a new economy, a new politics and government, and a new war. Drone warfare, in turn, gives rise to new phenomena at the psychological, social, and global level. At the individual level, we see that pilots and operators in the assailant countries have become susceptible to various psychological problems, while affected populations in targeted areas are suffering from anxiety and disintegration. At the social level, citizens of perpetrating countries have become desensitized to endless war through the mediated apathy of drone warfare, while traditional mechanisms of social cohesion in targeted areas are undermined due to fears of drone attacks. And, finally, at the global level, the sovereignty of independent nation-states is undermined by unsolicited attacks on their citizens, increasing the *real* prospect of the spread of drones as weapons of choice by state and non-state actors and elevating the fear of an unregulated, uncontrollable, and lawless environment on a global scale.

This chapter ends with a brief examination of these different types of disorder.

Psychological Disorders

Psychological disorders are prevalent on both ends of drone warfare: the assailants and the targeted populations. On the assailant side, observations and studies have shown increasing signs of psychological problems among drone operators or "pilots," who are stationed in one of the many US bases on American soil and outside. A typical day in the life of a pilot is something like this: He or she wakes up at home in Las Vegas, drives to the base, moves to one of the many Ground Control Stations (GCS) dedicated to this. The GCS is basically a mobile container, stacked

with a dozen or so monitors of different sizes. Some of the monitors display the video feed that flows from the very sophisticated cameras installed on the plane. Others provide live intelligence reports or chat rooms for the pilot to exchange information with ground troops or with the Central Command. This is where the pilot will spend the next 10–12 h flying an aircraft almost 6,000 mi away on the other side of the globe over Afghanistan, Iraq, Yemen, etc. During this time, he or she will be gazing on multiple screens, trying to understand the influx of video feeds, intelligence analysis, continuous chatter, etc. The typical mission can be described as "find, fix, and finish" – that is, to hover over a zone of interest, which is typically reported by ground intelligence as either a potential area of activity by insurgents or the living quarter of a prespecified target. On a "good" day, the pilot might manage to take one of these targets out, thereby completing the "find, fix, and finish" cycle, in which case they are expected to stay zoomed on the target in order to see the outcome and the carnage of the attack. Otherwise, they pass the operation to the next shift and go back home to resume a "normal" life with their family.

Lt. Colonel James Martin was one such pilot, and he has chronicled his experiences in detail and with great candor in his book: Predator (Martin and Sasser 2010). As a former fighter pilot, Martin is also in a position to provide very informed comparisons between what it means, and how it feels, to be a drone operator versus a fighter pilot. For instance, he highlights the issues of time lag between the GCS and the aircraft. Although only 2 s, the time lag is long enough to compromise the navigational capabilities of pilots, leading to frequent crashes during takeoff and landing.

Martin also highlights the challenges of a disembodied relation between the pilot and plane. From an operational perspective, the drone operator functions as a hub, a coordinating center where sensory information is brought together, interpretations and decisions are made, and action commands are dispatched back to the aircraft for execution. From an experiential and phenomenological perspective, however, the pilot has to compensate for the disembodied interaction with the plane and for the detached relationship with his targets. Martin, for instance, describes how he sometimes found himself crouching over to look over the nose of the aircraft.

Martin also provides some candid descriptions of the moral issues that he faced as a drone pilot, especially his perception of human beings "down there" from his position in the "god's seat," as he describes it himself:

> I was concentrating entirely on the shot and its technical aspects. Right range, right speed, locked in. The man wasn't really a human being. He was so far away and only a high-tech image on a computer screen. The moral aspects of it – that I was about to assassinate a fellow human being from ambush – didn't factor in. Not at the moment. Not yet.

A few points can be highlighted from this very brief sketch of the daily life of a drone pilot:

i. The dissonance that derives from daily transition back and forth between routine family life and combat operation and the *Compartmentalization,* which drives the need to separate "normal" family life from the deadly reality of combat operations.

ii. Disembodied engagement with the environment increases the chance of "errors," including crashes.
iii. Detachment from the operation theater and awareness of the nonreciprocal situation can create a false of sense of security combined with a sense of guilt.
iv. The boredom/frustration of gazing at screens without immediate outcome can lower the threshold of action and increase the possibility of overreacting in order to compensate for the fact that pilots know that they are not "there."
v. The assurance but also the trauma that comes from witnessing the carnage caused by drone attacks.
vi. The sense of superiority deriving from the God's eye view provided by sophisticated visual technology.
vii. A crisis of identity that they are not "real" pilots, sometimes called "joystick warriors" by their own peers, becoming the subject of ridicule (as shown in this cartoon). This is one reason why the term "drone" is unpopular among Predator crew members, many of whom wear patches that say, "We're not drones. . . we shoot back." (Cullen 2011, p. 18).

This combination of cognitive, psychic, and moral issues can give rise to mental and psychological states that might, in fact, constitute a novel condition. Reports and studies show the prevalence of some sort of psychological problem among these pilots, resulting in recruitment and turnover issues. Military psychologists and other experts disagree on how to categorize and evaluate these problems. While some of them categorize these as PTSD, others are skeptical, arguing that there is no trauma involved in what drones pilots experience. Dr. Hernando Ortega, a USAF surgeon, for instance, wonders whether the symptoms observed in drone pilots match "classic PTSD" descriptions. He also wonders how the aviation culture in the Air Force is going to come to terms with the status of the drone operator

> who no longer has a helmet; he no longer has a G-suit, A-tags, advanced equipment that's actually helping him now to do his job, because we're taking him out of that environment. So now this guy, basically the only thing he has left is the Nomex flight suit, which really gets to my whole issue of . . . the inertia around this aviation culture . . . who is going to be the high cultural status individuals in the warfare or in the military (Brookings 2012).

If drone operators are susceptible to these kinds of stress, tension, and perhaps trauma, individuals at the other end of drone warfare suffer from a different set of problems and issues.

Based on patterns of life analysis, numerous incidents of mistaken signature strikes have been reported, most famously the case of a convoy of Afghan villagers who were bombed early in the morning of April 10, 2011, leaving 23 dead and 12 other injured (Cloud 2011). The group first raised the suspicion of the drone crew because they had formed a convoy early in the morning. Here is part of the chat transcript between the drone operator and the image analysts that followed:

> "Our screeners are currently calling 21 MAMs [military-aged males], no females, and two possible children. How copy?" the Predator pilot radioed the A-Team at 7:38 a.m."Roger," replied the A-Team, which was unable to see the convoy. "And when we say children, are we talking teenagers or toddlers?"
>
> The camera operator responded: "Not toddlers. Something more towards adolescents or teens."
>
> "Yeah, adolescents," the pilot added. "We're thinking early teens."

Subsequent intelligence showed that the villagers, who consisted of "shopkeepers going to replenish their supplies, students going back to school, people going for medical treatment, families off to visit their relatives," were traveling as a convoy for fear of a vehicle failure or a Taliban attack. The disaster illustrates the potent and potentially misleading character of the label MAM (referring to military-aged males) as a basis of inference in drone killings.

The use of MAM is not an exception but part of a broader move toward basing military action on remote interpretations, which are allegedly made "situation aware" through sophisticated video, navigation, and data analytic technologies. What motivates the appeal to these representational technologies such as images, labels, data analysis, etc. is a demand to manufacture situational awareness in the absence of situatedness.

In October 2011, a marine staff sergeant and a navy medic who were first recognized as "friendlies" were subsequently judged to be insurgents and killed by drone fire. An investigation found the cause of the attack to be "a fatal mix of poor communications, faulty assumptions and 'a lack of overall common situational awareness.'"

After watching the drone feed, the father of the marine was quoted as saying "You couldn't even tell they were human beings – just blobs."

The moral dimension of these anecdotes are hard to dispute. Beyond the moral dimension, however, the kinds of disarray and disorder that can be triggered by these practices are not difficult to imagine. We don't have studies of the psychological effects of these types of strikes on individuals who might be somehow affiliated with an insurgent. What if you are the relative, say the brother, of a known insurgent? Or their classmate? Or a neighbor who happened to have shared a phone number with them? Or a taxi driver who took them to a destination without knowing who they are? Or someone who has once opened the door to a house that has later turned into a safe haven?

Societal Disorders

Beyond individuals, drone warfare cultivates a particular worldview that is heavily invested in the geographic, cultural, and technological distance between the two sides of the "war." And both sides of the drone equation are vulnerable to this epistemic chasm, albeit with very different costs. On the one hand, the layers of mediation generated through this distance give rise to, and feed off of, a kind of apathy that is amplified and mystified by the false sense of proximity offered by

digital technology. The cost here is complacency, indifference, and self-deception – the burden of which might not be immediately visible but runs a very high risk in the long run. On the other hand, we witness the disintegration of traditional communities and cultures in the targeted areas. The cost here is social disarray, conflict, and collapse – and, of course, human life.

Global Disorders

The majority of modern weapon systems (tanks, bombers, nuclear weapons, etc.) have high thresholds of acquisition, development, or operation because of their complexity, cost, or simply size. Drone technology, on the other hand, is relatively easy and inexpensive to acquire and operate. Therefore, they provide the prospect of quick expansion and spread around the globe. On the other hand, there is a vast gap between public views in the USA and the rest of the world toward drone warfare. While drones have become a political issue for the American electorate only in the last few years, they entered the political consciousness of affected populations early on. Absent drastic reforms, the US drone program will likely remain unpopular abroad, while the American public will remain more or less indifferent to and ignorant of foreign or even domestic employment of drones (Koebler 2013).

Legal experts point out the shortcomings of international law in dealing with the issues raised by drone warfare. Historically, international norms are established and reinforced through practical change and consent of states, rather than through legal frameworks. "Unlike treaties," Clark (2003) argues, "customary international law is not created by what states put down in writing but, rather, by what states do in practice." More poignantly, Ricks (2014) contends, "If we can't figure out whether or not there's a war – or where the war is located, or who's a combatant in that war and who's a civilian – we have no way of deciding whether, where, or to whom the law of war applies."

Based on the above assessments, commentators warn that the inability of international governing institutions to hold state and non-state actors accountable may ultimately destabilize the international system, putting us on a "slippery slope," lowering the threshold for the use of force, and increasing the risk of tit-for-tat escalation (Abizaid and Brooks 2014; Kreps and Zenko 2014). These concerns find material support in current initiatives around the world to expand drone technologies – e.g., the launch of the European Drone Club (Rettman 2013) and the joint UK-France program on Future Combat Air System (Cole 2014).

Conclusion

The emergence of drones as weapons of choice by the American military raises various political, ethical, and philosophical questions but also a historical question about the timing of this phenomenon. This chapter seeks to provide an explanation for this last question, providing a description of some of the broader economic,

political, and military changes of the last few decades as the backdrop. Economically, the development of a new spirit of capitalism on a global scale – what some commentators refer to as a "knowledge economy" – has set the stage for fast and personalized techniques of manufacturing, trading, and financial transactions. This new spirit finds a surrogate in drone warfare toward "personalized" surveillance, identification, and killing of enemy combatants in theaters of war but also in areas that are not officially declared as war zones. Growing poverty and the reduction of tax income for governments on both ends of the drone warfare also necessitates a new level of accountability and oversight over military spending. Drones suggest themselves as effective means of cost-saving in this regard.

Politically, the change in the character and role of modern states that govern at a distance, increasingly relying on private experts, consultants, emissaries, and missionaries, has prepared the environment for clandestine operations that target alleged enemies on the basis of their patterns of life. On the other side of the globe, this trend manifests itself in the declining power of central governments, which now have to share power with non-state actors on the local and global scene. In extreme cases, this has given rise to failed or rogue states that are not capable of providing security to their populations, providing justification for extraterritorial interventions by governments such as the USA and Israel, which step into the vacuum in the name of their own security.

Lastly, militarily the change to "new wars" is justified in terms of an asymmetric situation where, instead of nation-states fighting for victory and territory, combat is conducted between powerful states with advanced technology, on the one hand, and, on the other, individuals or organized groups fighting under the banner of an ideology.

It is in the convergence of these trends and developments that one can make historical sense of the current expansion of drone warfare, as well as the response to it. The outcome of the 2016 presidential elections and the emergence of new isolationist policies in the USA and elsewhere seem to reinforce, rather than reverse, these trends. Despite its differences with the previous administration, the new one is continuing the policy of drone warfare, only to reinforce it with traditional military spending. Whether or not this amounts to the emergence of a new spirit of capitalism is a question that needs to wait further developments in the USA and beyond.

References

Abizaid, J. P., & Brooks, R. (2014). *Recommendations and report of the task force on US drone policy*. Washington, DC: Stimson Center.

Boltanski, L., & Ciapello, E. (2005). *The new spirit of capitalism*. London: Verso.

Bourguignon, F. (2015). *The globalization of inequality*. Princeton, NJ: The Princeton University Press.

Braudel, F. (1977). *Afterthoughts on material civilization and capitalism*. Baltimore: The Johns Hopkins University Press.

Brookings Institution. (2012). *Combat stress in Remotely Piloted/UAS operations*. http://www.brookings.edu/~/media/events/2012/2/03%20military%20medical%20issues/0203_military_medical_issues.pdf

Chamayou, G. (2015). *A theory of the drone*. New York: The New Press.
Clark, A. (2003). International law and the preemptive use of military force. *The Washington Quarterly, 26*, 89–103. The Center for Strategic and International Studies and the Massachusetts Institute of Technology.
Cloud, D. (2011, April 10). Anatomy of an Afghan war tragedy. *Los Angeles Times.*
Cole, C. (2014). UK-France declaration reveals new reaper users club to rival European drone club. *The Guardian*. Web.
Congressional Budget Office. (2015). *The budget and economic outlook: 2015 to 2025*. Washington, DC: Government Printing Office.
Cullen, T. M. (2011). The MQ-9 Reaper remotely piloted aircraft: Humans and machines in action. Doctoral Dissertation, Massachusetts Institute of Technology.
Ekbia, H., Matiolli, M., Kouper, I., Arave, G., Ghazinejad, A., Bowman, T., Suri, R., Tsou, A., Weingart, S., & Sugimoto, C. (2015). Big data, bigger dilemmas: A critical review. *Journal of American Society for Information Science and Technology, 66*(8), 1523–1746.
Fallows, J. (2015, January/February). The tragedy of the American military. *The Atlantic.*
Gongloff, M., Hall, K., & Diehm, J. (2013, September 10). 5 years after the crisis, big banks are bigger than ever. *Huffington Post*.
International Human Rights and Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at Nyu School of Law, Living Under Drones. (2012). *Death, injury, and trauma to civilians from us drone practices in Pakistan*.
Kaldor, M. (2006). *New and old wars: Organized violence in a global era*. Palo Alto: Stanford University Press.
Koebler, J. (2013, May 28). Poll: Americans OK with targeting citizens overseas. *US News and World Report.* Web.
Kreps, S., & Zenko, M. (2014). The next drone wars: Preparing for proliferation. *Foreign Affairs*. Web.
Martin, M. J., & Sasser, C. W. (2010). *Predator: The remote-control air war over Iraq and Afghanistan: A pilot's story.* Minneapolis: Zenith Press.
Miller, P., & Rose, N. (2013). *Governing the present*. London: Polity Press.
Rettman, A. (2013). Seven EU states create military drone 'club'. *EU Observer.* Web.
Ricks, T. (2014). The future of war: Some questions for considering in light of changes. *Foreign Policy.* Web.
Stiglitz, J. (2014, June 29). Is inequality inevitable? *New York Times*.

Space Defense: A New Offensive

16

Boris S. Manov

Contents

Abstract

In the beginning of the century, science fiction depicted cyber and space weapons as fiction. Nowadays the fiction is turning into reality and more and more technology is being created for the sake of "defense." Only three states in the world have the capacity to research and develop such means of contesting outer space. This analysis will look into the current USA, Russian, and Chinese space policy and cyber development, which might lead to a potential outer space conflict in the near future.

B. S. Manov (✉)
Political Science, Researcher at University of Vienna, Vienna, Austria

Sofia, Bulgaria
e-mail: boris_manov@hotmail.com

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_61

Keywords
Cyber defense · Space defense · Cyber development · Space technology · Cyber democracy · Space warfare · Space offensive

Introduction

The space race, during the last century, showed humanity the ingenuity of science. Twenty-six years after the Cold War, humanity is on the brink of another space race. This competition, just like the last, has essentially a strong military character behind it. Nonetheless the number of competing nation states has grown. Besides the conventional USA and Russian presence, China too has entered the space contest. The United States, Russia, and China are the only three countries, able to endure in a space race. The three superpowers have the economic capacity to pursue alone new methods of acquiring power in the outer space, without relying on third parties (Anantatmula 2013, p. 133). The well-established US dominance of the skies has prompted the other two nations to develop symmetrical and asymmetrical methods of challenging the traditional hegemon and attempting to gain a strategic advantage in the high ground. Taking the perspective that outer space has been already militarized (Wolff 2003, p. 6), I shall construct my argument upon the focal points of the theory of realism. The analysis intends to consider the three superpowers as the central actors to the weaponization of space-based technology and portray the destabilizing effect that would pose to the international system. Columba Peoples elaborate more on the inevitability of a conflict in space "One commonly offered basis of the inevitability thesis is human nature, the idea that weapons and war inevitably follow from the naturally bellicose character of human beings, which will apply as much in space as in any other dimension." (Peoples 2008, p. 504). We shall try to interpret certain features, which support the idea of a new space race between the United States, China, and Russia. The changes in the military space policy of the nation states and the wide range of counterspace capabilities developed will highlight the growing importance of controlling the high ground as an economic and military strategic advantage. Securitization of outer space can lead to weaponization. Likewise a space defense can essentially become a space offense. The cyber-development and cyber-defense will play vital roles in the near future, when space will be assumed as the ultimate contested area.

Schools of Thought

Within the last 50 years, scholars came up with two schools of thought, when we discuss the use of outer space. Contrasting each other, both schools point to outer space as the inevitable future step of human development. The first, the internationalists, believe space should be a safe sanctuary and no weapons should

be positioned in outer space. Led by James Moltz Clay, the internationalists advocate the use of space for scientific, commercial, and peaceful purposes (Moltz 2008, p. 23). In addition, they believe that states can cooperate together for the common good and overcome the final frontier without any militarization of outer space. However, such a vision could be taken as naive, when history has shown numerous times, the struggle for power in the international realm between the nation states (Pavelec 2012, p. 41). This viewpoint is idealistic and also very hard to imagine, given the current geopolitical situation on Earth and the diminishing economic resources. Hence, comes the argument of the realists, who posit the inevitable exploitation of the space common, based on the pursuit of their national interests. Essentially, the international system is anarchic and nation states within this system have to take care of themselves (Waltz 1979, p. 10). Survival and dominance, through military capability, are the foremost intentions of a nation state (Mearsheimer 2001, p. 3). Moreover, they endeavor to gain maximum economic benefit and extend their efforts to project power in space, just like any other domain. Morgenthau posits "States pursue their national interest agenda in consonance with their natural resources, geography, ideology, and capabilities" (Morgenthau 1948). In other words, they act rationally in accord to their desires for obtaining power. In the new age of information, dominance of the high ground or the outer space is the key component to guaranteeing a strategic advantage over the adversaries. Putting emphasis on states as the central actors and their interests as core motivator for actions, the realist viewpoint, explains much more suitably cyber defenses and space weapons. Concurring with the realistic paradigm, in this multipolar world, outer space as any other sphere of dominance, land, sea, air, should be taken advantage of as a necessary prerequisite to obtaining or maintaining power. According to Everett Dolman, the competition of the Cold War, the realpolitik, is what drove forward the innovation and development of space as a key component (Hickman and Dolman 2002, p. 3). In his discourses, Dolman believes the United States best be the initiator of defensive space armament, as the champion of democracy and liberal peaceful ideas (Dolman 2001). This way, Dolman considers peace and stability to be ensured, by the United States, which is the biggest and most advanced space power. Assuming again a realist perspective and a deterministic view, it is normal that other capable nation states, such as Russia and China, will seek reciprocal measures. Protecting vital economic and informational assets and projecting military dominance are the key components, which stand behind the defensive rationale of the three superpowers. Controlling Earth's orbits has become the ultimate advantage, towards which they are striving. According to the military space doctrines, scholars classify "Sanctuary" as the first level of space weaponization, with no weapons present at that stage. High ground, contrary, has the highest level of weaponization (Sadeh 2003, p. 343). Regarding outer space as the ultimate high ground inevitably will lead to the congestion, competition, and contestation, by nation states able to do so (Sariak 2017, p. 52). Peoples give a good account of the difference between militarization and weaponization, "Space militarization generally denotes the use of space-based technology and infrastructure for the purposes of supporting military operations and functions including: reconnaissance, navigation, and use of satellite

targeting systems for terrestrial weapons. Space weaponization is usually refers to the actual placement of weapons in outer space" (Peoples 2011, p. 76). Technological assets, such as satellites, are militarized and vital to the communicational networks of modern warfare and as such need to be safeguarded at all costs (Honkova 2013, p. 25). Satellite reliance presently is a vital component to the communication between the military structures, institutions, and facilities of a nation. In line of this thought, defense and weaponization of space-based technology becomes inevitable, to protect the network capability from harmful interactions (Sariak 2017, p. 59). The rationale for defending and preserving technological assets in outer space will be the pretense for installing diverse set of weapons, which could simultaneously possess offensive capabilities. International treaties remain vague upon the notion of outer space weaponization; therefore, numerous of new cyber and space defense technologies are developed, which might not be classified at all as weapons, but still have a harming potential. Moreover, this lack of a clear definition of what a weapon in space constitutes and allows defense technology with counterspace capabilities to be installed on space-based assets. Such advancements in the militarization of space could pose detrimental consequences to conflict escalation and peace stability (Peoples 2011, p. 78).

The Double Ds

There are two big terms, which induce cyber defense and the defensive weaponization of space. These are determinism and deterrence. Each of them influences the course of action of the superpowers and is applied to justify further cyber development of counterspace capabilities. Under the realistic paradigm, in philosophical terms, determinism applies to the cause and effect of states responding to the development and deployment of each other's military space capability (Hoefer 2008). If the United States starts to build up their counterspace capabilities, China and Russia will pursue the same to balance the power. Under technological determinism, technology and science are stressed as the main elements to decision-making regarding outer space (Moltz 2008, p. 28). In the words of Michael Pavelec "This [technological] determinism includes the opinion that technology—in this case, space technology—will eventually contribute to changes in society and international relations. Those countries at the leading edge of technological development will enjoy advantages for the foreseeable future" (Pavelec 2012, p. 42). This position explains the reciprocal relationship in developing and proliferating cyber defenses among the three space powers. The second term, deterrence considers preventative weaponization for ensuring survivability. According to Schelling and his work on the Deterrence theory, it is argued that military strategy has transformed into the art of deterrence. In the Deterrence theory, a state's capacity for inflicting harm prevents the other states from acting against it (Schelling 1966). Russia, China, and the USA all use deterrence against each other, to maintain the balance of power and check each other's desires of achieving world dominance. And while many scholars and officials, such as Henry Kissinger, have become proponents to arms disarmament (Goddard 2010), maintaining the

largest military defensive budget and being the most prominent innovator in science and space technology, the US military space policy shows tendency to favor advocating counterspace capabilities and new types of antisatellite attacking technologies (ASAT), with the justification of safeguarding and defending vital strategic space assets. Deterrence and Determinism go hand in hand as the primary motivators for weaponization and securitization of outer space. We can also presume that if another space race follows, it can greatly increase the research and development in the sphere of outer space technology. The benefit of a space race clearly lays in faster technological progress; the human race can undergo; however, the downside is the increasing risk to the stability in the international relations between the superpowers. Likewise Sariak posits "The paradox is that the stability military space technology can provide, as well as the benefits states can derive from its use, engenders a security dilemma whereby states pursue active military space technology to end the advantage for the powerful spacefaring states" (Sariak 2017, p. 61).

United States

US Military Space Policy

In 1998, through his report "On Space Warfare," Lt. Col. David Lupton puts forth the notion of four different military doctrines regarding space, deriving from the realist school of thought. Besides the traditionally accepted "Sanctuary": "Survivability," "Control," and "High Ground" were introduced (Lupton 1998, p. 19). By measuring the level of weaponization of space, the US military decides and adopts what types of space defense technology it would deploy (Sadeh 2003, p. 341). The "Sanctuary" concept is very related to Deterrence theory. Allowing deployment of space systems to verify and early-warn against a possible first strike lets outer space be considered as a safe domain (Lupton 1998, p. 32). Technological determinism has played an important role in US military space policy and still does today. Identifying outer space as critical to maintaining economic and military superiority, the USA have shaped their space policy along the lines of their national interests.

The Bipolar World

At the end of WWII, American military scholars realized the potential of outer space as a strategic advantage over adversaries. Both the USA and USSR had developed means of destruction, which utilize air space and outer space. The "Sanctuary" doctrine was first proposed by Eisenhower in his open-skies speech for a weapon-free space and satellite verification of early-attacks (Lupton 1998, p. 20). This policy eventually allowed for the first militarization of space, by allowing military-controlled satellites to be sent to outer space for reconnaissance and surveillance (Armstrong 2014, p. 77). The launch of "Explorer" following "Sputnik" is an example which demonstrates the technological determinism that fueled the Space Race. Another good example is the Anti-Ballistic Missile systems. After, Washington discovered Soviet plans to construct an ABM system in Estonia in

1962, the US military responded in a symmetrical fashion proposing their own defense system. Recognizing the destructive capabilities of WMD's combined with the strategic advantage that outer space provides, treaties were signed to ensure peace and stability. The Outer Space Treaty (OST) of 1967 and the Anti-Ballistic Missile Treaty (ABMT) of 1972 were ratified by both countries to halt further arms proliferation of outer space (Peoples 2011, p. 77). In the early 1980s, in accordance to the introduction of the other three military space doctrines, at the Air University's Airpower Symposium (Lupton 1998, p. 19), Ronald Reagan initiated the Strategic Defense Initiative (Podvig 2013, p. 1). Although it remained only a proposed project, the inability of the Soviet scientists to compete with their US counterparts in advanced technologies led to Moscow seeking negotiations to halt any further progress on the SDI and any other space weapons (Podvig 2013, p. 4). The strive for military space superiority in the bipolar world ultimately led to the demise of the USSR and the ascension of the United States as the space hegemon.

Remaining a Hegemon

Throughout the 1990s, the US military began openly using their space-based assets to their strategic advantage in Desert Storm and the conflict in ex-Yugoslavia. In his essay, Dwight Day posits "Desert Storm is often referred to as the 'first space war' where satellites played a significant role in the conflict" (Day 2003, p. 385). Besides providing important data through reconnaissance, surveillance and navigation, satellites were used to direct precision-guided missiles (Hamilton 1995). In addition to utilizing space as a strategic advantage, US military has identified space as economic center of gravity, essential to US national interests. In his essay, Peter Hays postulates "Although the notion of space as a sanctuary appears seductive to many, our increasing reliance on space systems and information derived from space, creates a center of gravity potential adversaries clearly understand. Protection takes on a new dimension as non-DOD systems (commercial and third-party) become even more integrated into plans for using joint forces" (Hays 2003, p. 351). After 9/11, with the pretext of defense and securitization of space, the Bush administration withdrew from the ABM Treaty, allowing the USA to start working on a Ballistic-Missile Defense (BMD) with orbital weapons (Spacy 2010, p. 1). George Sariak discusses "Since a limited strike is out of the question, and mutually assured destruction (MAD) accompanies a full strike, BMD has the power of limiting the ability of states to use their ballistic missiles as a diplomatic tool to gain greater influence and power" (Sariak 2017, p. 56). Creation of a BMD highlights how deterrence theory is used in retrospect to weaponization and space defenses. The US National Space Policy of 2006 underscored how United States national security is dependent upon space capabilities and that this dependence will grow (FAS 2006, p. 3). Consequently Chinese ASAT tests in 2006 and 2007 further raised US awareness for securitization. This notion of securitization was again highlighted in the 2011, US National Space Security Strategy "Space is vital to U.S. national security and our ability to understand emerging threats, project power globally, conduct operations, support diplomatic efforts, and enable global economic viability" (US DOD 2011, p. iii). As the leading space faring state out of the three

superpowers, USA needs to sustain their superiority in space. The United States spends as of 2017, $582 billion on defense (US DOD 2016). Moreover, a report by OECD shows that the USA spends more than the next ten countries combined in the ranking on space programs and R&D (OECD 2014, p. 18). It must be also duly noted that the total defense budget allocated goes to more than 15 federal agencies managing the national security. "The major organizational stakeholders in military space include DOD, the Navy, the Army, the NRO and the Intelligence Centre (IC), the Air Force, the Air Force Command and US Space Command" (Hays 2003, p. 345). Each agency helps the US military form a national defense strategy and policy, all being run through the Department of Defense. As of 2017, new plans have been put forth to create a dedicated Space Corps, dealing exclusively with space. The proposed duties are: "protecting the interests of the United States in space, deterring aggression in, from, and through space, providing combat-ready space forces that enable the commanders of the combatant commands to fight and win wars, organizing, training, and equipping space forces and conducting space operations of the Space Corps under the command of the Commander of the United States Space Command" (Subcommittee on Strategic Forces 2017, p. 5). Such structural changes indicate optimization of the US space institutions, with the goal of enhancing American defense of space technology.

U.S Space-Based Defense Technology

"The United States is the leading country in outer space technologies and the sole country in the world that has translated its space assets into war-fighting capability in practice" (Chunsi 2008, p. 624). Moreover, "The decision to weaponize space does not lie within the military (seeking short-term military advantage in support of national security), but at the higher level of national policy (seeking long-term national security, economic well-being, and worldwide legitimacy of US constitutional values)" (DeBlois 1998, p. 41). Furthermore, DeBlois writes in another work "Civil and commercial interests in space are rapidly outpacing military concerns and are becoming a central focus for many national economies. As a service to the state, the military role is typically to organize, train, equip and posture forces—complete with weapons—to defend those interests. Space weapons will necessarily follow space commerce—that is, they will follow the money" (DeBlois 2003, p. 32). Clearly stating the importance of space-based technology on the economic and strategic advantage, the USA has developed both symmetrical and asymmetrical cyber defensive technologies and systems to demonstrate commitment to protecting those national interests and their space hegemony. Concurring with Peoples, besides the conventional satellite reconnaissance and nuclear missile proliferation, the US military "conducts research into more exotic forms of space weaponry, and funds a variety of technologies aimed at creating a force application capacity from space" (Peoples 2011, p. 84). Deterrence and technological determinism has prompted the USA to also develop asymmetrical responses to balance the threat, from new Russian and Chinese antisatellite attacking technologies.

Satellites and Ground Infrastructure

In the words of Bruce DeBlois, "Space-based imaging capabilities, with their origins in the Cold War satellite photography, are now crucial element of defense complexes." Moreover "Digital remote imaging with near-real-time intelligence capabilities allows for the persecution of time-critical targets" (DeBlois 2003, p. 36). Hence, the US government operates the largest fleet of civilian and military satellites providing military information superiority and military operational superiority over their adversaries (DeBlois 2003, p. 36). According to the Union of Concerned Scientists, there are currently 1,459 satellites orbiting Earth, out of which, 593 are American (UCS 2017). The GPS, one of the most famous military inventions, serves as the neural network providing navigation, timing and positioning for commercial, civilian, and military uses (Hays 2003, p. 360). Furthermore, US military satellites are used for missile detection, communications, radar imaging, surveillance, optical reconnaissance, and scientific research (Krebs 2017). Such comprehensiveness of satellite activity helps the USA to maintain the strategic advantage of the high ground and preserve national security interests laying in space-based assets. Likewise to maintain this large space presence, the US government uses numerous of launching rocket sites, for deploying satellites, testing ballistic missiles, as well as initiating manned and unmanned missions. According to SpaceToday, the ground infrastructure composes of more than 20 space launch facilities both for civilian and military launches, some of them operating since the end of WWII (SpaceToday 2017). Recognizing the vitality of this massive space infrastructure has prompted the US military to develop synchronously many methods of defending these space-based assets.

ASAT Systems

Despite regarding outer space as "Sanctuary," the US military tested their first missile ASAT weapon, the "Bold Orion" in 1958 as a direct response to the "Sputnik" launch. It essentially carried a nuclear warhead, but it was deemed inefficient, due to its sheer destructive power to any space-based assets (Armstrong 2014, p. 71). Nowadays building upon that conventional missile ASAT concept, the USA still maintains and modernizes constantly the largest arsenal of nuclear warheads installed on ICBMs (ACA 2017). Nuclear deterrence still plays an important role in balancing the threat of other nations developing, symmetrical methods of counterspace capability. Yet besides the development of ballistic missiles and ballistic-missile defenses, the US military has promoted asymmetrical methods of counterspace capabilities, which include laser and kinetic ASAT weapons. The first ideas about using lasers as defensive systems came during the Reagan administration, with the Strategic Defense Initiative in the 1980s (Peoples 2011, p. 84). William Spacy writes "Since light has no mass, lasers are not constrained by orbital dynamics and can fire against any target within their range and line of sight, hitting it almost instantaneously" (Spacy 2010, p. 3). Last year, 2016, the *Small Arms Defense Journal* reported the installation of a Laser Weapon System (LaWS) onboard the Navy's assault ship USS Ponce. Rear Adm. Matthew L. Klunder stated "Laser weapons are powerful, affordable and play a vital role in the future of naval combat operations" (SADJ 2016). In

regards to the second type of an asymmetrical counterspace capabilities, Spacy notes "Alternative weapons that physically impact their target are more feasible given current technology. These weapons either use the kinetic energy of a direct impact, or pass near enough to a target for an exploding fragmentation device to destroy it." (Spacy 2010, p. 9). Peoples also confirms, "The Department of Defense has reportedly explored several high concept space weapons systems such as Hypervelocity Rod Bundles (tungsten rods dropped on targets from space that would theoretically use gravity as accelerant in a manner akin to a meteor, or Rods from God)" (Peoples 2011, p. 84). Drawing upon these ingenious concepts, the US military has also proposed a third type of an exotic technology, the co-orbital ASAT. The system functions with a co-orbital vehicle which nears another space-based asset and then destroys it with an exploding warhead (Spacy 2010, p. 10). Interestingly enough the US Air Force has such a vehicle, named X-37B Orbital Test Vehicle, testing reusable technologies as a space platform (AF 2015). The technological determinism and the development of such a wide array of symmetrical and asymmetrical counterspace capabilities underscores the notion of securitization. The weaponization under the pretext of securitization has been instigated to defend economic and national security interests, against the other two space powers, China and Russia.

Russia

Russian Military Space Policy

As a whole we can divide the development of the Russian military space policy into three periods. During those periods, the outlook towards how should military space policy be conducted shifted twice. The strategic outlook on what type of military space policy must be implemented always depended on the complex interactions with the other superpowers. For the Russians, there are two ways of perceiving strategic thinking, the traditional Soviet offensive one and a defensive one that followed the breakup of the Soviet Union (Mowthorpe 2002, p. 27). Each of the schools of thought was based on determinism and its approach for its respective time.

Soviet Era

In the beginning of the Cold War, recognizing the vitality of air and outer space as a strategic advantage and a force multiplier, USSR began contesting it (Honkova 2013, p. 40). Aerospace supremacy was evidently going to be the next level of conflict. Well aware and possessing offensive military strategic thinking in terms of military policy, the USSR successfully challenged the USA, for many years (Mowthorpe 2002, p. 26). Being the first to send a satellite in space ("Sputnik"), the first to start developing an ABM complex (near Tallinn, Estonia) and the first to send a man to space ("Yuri Gagarin") could be best depicted as examples of strategically offensive thinking, to gain more prestige or acquire more power in the international realm. On the other hand the Soviet Union knew that their technological innovations and economic capacity are inferior to their rivals; thus, they sought

other means of restraining the US attempts at armament. On the diplomatic level, through soft power, the Soviet Union ratified a numerous treaties during the Cold War, including the Outer Space Treaty, the ABMT, and the Strategic Arms Limitation Talks (SALT II) of 1979. This way the Soviets managed to keep American ambitions for weaponization of outer space in check, by putting a global pressure on them, to agree to nonproliferation and reduction of arms production (Anantatmula 2013, p. 146). The latter mentioned agreements signed since 1972 posit how Soviet mentality started to alter towards a defensive standpoint. Nevertheless, Russia continued to fund experimental R&D projects for space-based technology, until the disintegration of the USSR in the early 1990s (Shoumikhin 2002, p. 96).

Turbulent Aftermath

When the Soviet Union collapsed, it underwent major structural and institutional reforms. The economic collapse suffered could not support the immense space industry that was created in the decades before. Lack of finances and confusion over ownership of launch facilities, such as Baykonur, brought further chaos in the new Russian Federation (Mowthorpe 2002, p. 26). Around two-thirds of the space programs were cut funding (Mowthorpe 2002, p. 41). During Soviet times, Politburo had promoted various programs, projects, and technologies ranging from ASAT lasers to signal-intelligence reconnaissance systems and consequently needed to cut their funding (Anantatmula 2013, p. 146). Only defensive and support mechanism were left in place. Offensive operations were substituted with defensive discourses, and the space industry took a step back (Honkova 2013, p. 4). Additionally the Russian Federation knew they could not maintain challenging the United States in the aerospace; thus, they tried to restrain them, using the previously signed international and bilateral treaties. This mode of defensive thinking persisted all throughout the Yeltsin presidency, until the Bush administration pulled out of the ABMT, and Russian suspicions were affirmed with the NATO expansions in 1999 and 2004 (Shoumikhin 2002, p. 101).

Dawn of a New Century

Since the early 2000s, the Russian Federation once again shifted its mentality to strategically offensive in terms of military space policy and acquiring power in the international realm. Russian military scholars began prioritizing yet again offensive over defensive operations (Vorobyov and Kiselyov 2007). According to Gen. Kornukov, “Experts believe that the side with aerospace superiority will have the initiative in any such wars and that ensuring superiority over the enemy in the aerospace field will be a necessary condition for achieving the objectives of the war” (Kornukov 2001). Under the Putin administration, the Russian Federation created a coherent military doctrine, which outlines the high ground as the key component to victory in contemporary warfare and outer space as the area most likely from which a threat to their security can be posed (Russia Embassy UK 2015). Elsewhere the notion of gaining supremacy over the skies and their adversaries have caused optimization and reforms in the Russian military forces, to adequately respond to the new environment. The military forces responsible for space underwent

sufficient mergers and reforms since the Cold War. Before 1992, they were designated as the Military Space Forces (MSF). After 1992, they were incorporated into the Russian Air Force, which also underwent structural changes only to be combined with the Russian Aerospace Defense Forces (VVKO) in 2015, to create the Russian Space Forces (Shoumikhin 2002, p. 103). Even before the transformations, Putin stated in 2012 during a meeting, the vital need for the VVKO, to integrate all air defense and aerospace assets, which are not under their control (Kremlin 2012). Currently 150,000 people are under service of the Russian Space Forces (IISS 2014, p. 181). It is said that further 200,000 are employed in the national space industry sector (Ionin 2006, p. 2). Such high numbers indicate a strong government interest in maintaining and improving their aerospace sector. Additionally a rising expenditure in the military sector in the last 18 years shows an increased interest from Moscow to compete with the USA (Stockholm International Peace Research Institute 2016). The military defense budget allocated for 2016 was $34.8 billion dollars, and for 2017 it has been boosted by another nine billion, up to $43.8 billion prioritizing upgrades and modernization of the military forces (TASS 2016). The new offensive military space policy, the optimizations of the structures operating space assets, and an increased spending in the defense sector indicate that the Russian Federation highlights control and command of aerospace as the key components to victory in contemporary warfare (SRAS 2010).

Russian Space-Based Defense Technology

Creating a precise national space defense strategy and policy helped to identify, which programs needed additional funding and which R&D projects needed to be pursued. Since the Cold War, Moscow has pursued symmetrical measures in weaponization against the USA. Development of ABM systems, ICMB missiles, and satellites for reconnaissance and surveillance are all conventional symmetrical methods of militarization. To be able to deter the USA and preserve a strategic advantage, Russia continues to upgrade and maintain a big nuclear arsenal (Shoumikhin 2002, p. 102). Besides the traditional means of weaponization, the Soviet Union pursued other asymmetrical responses to the US supremacy. Electronic, laser, and kinetic ASAT systems are all unconventional means of new space-based technology with the purpose of power acquisition and a change in the balance of power. In most of the cases, this power acquisition means heavy weaponization to use deterrence against the opponent. The theory of deterrence stems from the massive nuclear warhead proliferation during the Cold War. The same theory is applied, when amassing space-based weapons or space defenses. Thus, Soviet usage of symmetrical and asymmetrical responses, when creating space-based defenses, inclines comprehensive diverse set of technologies, with counterspace capabilities. Dave Webb contemplates “as more states obtain or develop missile technologies that could also have ASAT capabilities, weaker space power actors may decide to employ space weapons in an attempt to counter the advantage space confers powerful states” (Webb 2015, p. 116). According to him, asymmetrical responses will be pursued by

inferior states, which would accelerate space weaponization, which contemplates to a quicker escalation of conflict in outer space.

Satellites and Ground Infrastructure

Jana Honkova gives a good account of the main Russian satellite functions. She posits they are grouped into five categories: early warning, signal intelligence, optical reconnaissance, positioning, navigation, and timing (PNT), and communication (Honkova 2013, p. 10). Such an extensive array of satellites with diverse functions is supported by 15 types of satellite families, which need to be maintained and replaced constantly in order to help Moscow monitor any suspicious US or Chinese activity. GLONASS, the equivalent to GPS, gives Russia an alternative and independence to the US communicational dominance in space. In this modern age, information and communication stand vital to gaining an advantage over the rivals. Moreover, Bruce MacDonald recognizes the "Growing and vital role that space plays in modern life, the world has an overriding interest in maintaining the safety, survival, and function of space assets so that the profound civilian, commercial, and military benefits they enable, can continue to be available" (MacDonald 2009, p. 17). Besides the wide array of satellites with different functions, Russia built during the Cold War a complex network of launching sites and operational facilities, with some of the largest and most developed at Baykonur, Kaputsin Yar, and Plesetsk (Mowthorpe 2002, p. 26). As of 2018, the newest cosmodrome Vostochny is supposed to become operational and lessen the dependence on using the Baykonur, which ended up in Kazakhstan after the Cold War. Independence of launching military space operations will allow the Russian Federation to gain more power in contesting the outer space. And although the end of the Cold War left many facilities underfunded and obsolete, such as the Plesetsk cosmodrome (Honkova 2013, p. 33), the ground infrastructure that was built during the Soviet era remained intact, and only as of recently, plans have been developed to start modernizing and upgrading existing technology. In 2013, the newspaper *Izvestia* revealed new plans for a new ground global satellite intelligence system. This new ground infrastructure should integrate all previously built technological assets and facilitate operation costs related to space-based activities. Moreover, according to the newspaper "Akvarel. . .will be subsequently equipped with military radar, radio-technical and visual intelligence systems as well as other advanced systems" (Honkova 2013, p. 14).

ASAT Systems

ASAT weapons serve the purpose to deny, deceive, degrade, disrupt, and destroy (Anantatmula 2013, p. 134) adversary assets, and they show the willingness of a country to contest, congest and compete (Sariak 2017, p. 52) in space with other rivals. Russia is the first country in the world, to successfully develop a system with counterspace capability. In the words of Pavel Podvig "The Soviet Union was the only country that developed and operationally deployed an anti-satellites system (ASAT), designed to attack satellites on low Earth orbits (LEO)" (Podvig 2004, p. 126). According to Honkova, "It used the Tsyklon 2 (SL-11) carrier vehicle with

HE-fragmentation warheads that were placed into the same orbit as the target. The warheads were then gradually drawn closer to the target and eventually destroyed it" (Honkova 2013, p. 35). Besides the traditional symmetrical responses to weaponization, "the Soviet Union's directed energy weapons (DEW) were justified as an asymmetric response to the U.S. Strategic Defense Initiative (SDI)" (Anantatmula 2013, p. 147). Example of such a laser ASAT system was the Sokol-Eshelon installed on a jumbo jet meant to counter the infrared opto-electronic assets of the adversary (Honkova 2013, p. 37). During the Cold War, Soviet scientists developed a "Kontakt" kinetic ASAT system. It is meant to be deployed at an altitude of 1500 km by a MiG-31 and carries a high-altitude kinetic interceptor 79M6. Although the program was discontinued in 1989, the radar optical complex on the ground is still operational. Also it is rumored that replacements for the old 79M6 kinetic missiles are being developed (Honkova 2013, p. 38). Besides the latter two, Moscow is creating a new electronic defense weapon. According to the Russian agency TASS, "the Radio-Electronic Technologies Group (KRET) is developing a fundamentally new electronic warfare system capable of suppressing cruise missile and other high-precision weaponry guidance systems and satellite radio-electronic equipment." Additionally the CEO of KRET has stated, "[The weapon] It will fully suppress communications, navigation and target location and the use of high-precision weapons" (TASS 2015). Space-based technologies with offensive capabilities underscore Russian military thinking, which prioritizes offense than defense currently, as well as asymmetry along with symmetry. Concurring to Mowthorpe, "Russia appears to be developing its military along the lines of utilizing space as a further arena in which to conduct war" (Mowthorpe 2003, p. 44). The creation of new military counterspace capabilities in the ASAT systems, under a defensive pretext of space-based technology protection, can potentially lead to weaponization of space and have a destabilizing effect upon the balance of power.

China

Chinese Military Space Policy

Chinese military space policy has undergone two phases since the 1950s. According to Tang Shipping, we can divide the periods into two: the first was portrayed by an offensive realism strategy during the reign of Mao, and the second is referred to as defensive realism strategy, which substituted the former, with the newly appointed Deng Xiaoping. The two schools of thought in the realism camp differ in such ways that offensive realism refers to the inevitability of a conflict. Defensive realism on the hand highlights that beside a conflict, cooperation can take place between rivaling nation states (Shipping 2008, p. 12). Both schools of thought emphasize a realistic viewpoint, which recognizes China and its trailing position compared to the other space powers, USA and Russia.

China During the Cold War

China entered the space race in 1956, with their own nuclear program (Chunsi 2008, p. 622). Although intended originally as a reciprocal measure to the US and Soviet nuclear armament, gradually the space program took its own path. The first Chinese interest in developing technology and expanding their sciences began in the 1920s, when scholars highlighted technology as means to achieving superiority in the international realm. Concurring with Chunsi "Deng Xiaoping regarded science and technology as the chief productive force. The present Chinese leadership under Hu Jintao stresses the scientific outlook on development and the need to pursue an indigenous programme for the development of science and technology" (Chunsi 2008, p. 622). Such developments in science are noted by the initiation of "Project 863," which focuses on bio-technology, telecommunications, information and laser technology, new materials, automation, space, and energy. Originally started in 1986, it was a direct response to the defense missile system, SDI, initiated by the USA (Chunsi 2008, p. 623). Likewise to their Soviet counterparts, the Chinese have recognized the strategic advantage that air and outer space can provide, and have focused on developing their own space defenses and systems for early-warning (US DOD 2000, p. 14).

China Today

The Chinese military space policy today is divided into a short-term strategy and a long-term strategy, projecting defensive realism, based on the present geopolitical climate of US dominance in outer space. The short-term strategy aims to defeat US conventional forces, if a conflict escalates over Taiwan or in a close vicinity to the Chinese regional borders. The long-term strategy aims to challenge the United States geopolitically on a global scale (Tellis 2007, p. 45). Chinese military scholars recognize that "Based on American political, economic, and military influence, it is feared that Washington might attempt to contain the [People's Republic of China's] rise, particularly through strategically encircling it" (Chambers 2007, p. 9). Chinese interests lay mainly in safeguarding and protecting the economic advantages of utilizing a space program, especially satellites providing vital data (Chunsi 2008, p. 626). Providing a defensive rationale, Beijing tries to justify any space defense technology they might research. According to Ashley Tellis, "For China to sustain its high 'economic growth, preserve internal stability, and neutralize the external threats to its national security', space technological development is the key factor that strengthens military strategy at regional and international levels" (Tellis 2008, p. 2). Again Tellis postulates in her work "Mary FitzGerald. . ..has declared forthrightly that 'for more than a decade, Chinese military strategists and aerospace scientists have been constructing a blueprint for achieving space dominance'. This assessment concludes that the Chinese vision of space warfare involves not just denying space to its adversaries but using space for affirmative ends such as the intercept of ballistic and cruise missiles through space-based combat platforms; strikes by space systems on terrestrial targets; and attacks by land, air, sea, aerospace and space vehicles on an adversary's space platforms and space-based command and control assets and their associated terrestrial nodes" (Tellis 2007, p. 52). Coming

from a scholar [Fitzgerald], writing for the US Department of Defense, it might be a bit overstretched. However, there are numerous of Chinese scholars who confirm the same opinion as their colleague "Chinese military writings emphasize the need for dedicated space forces and for advanced space weapons and support capabilities designed to prosecute the full spectrum of 'space safeguard', 'space support' and '[space] attack' operations" (Pollpeter 2005, p. 334). Such actions could only be conducted by a dedicated military force, exclusively managing space defense. As of 2013, Beijing has started conducting reforms on the People's Liberation Army, planned to last until 2020. Reducing the size of the army, optimizing the army through restructures and modernization of the equipment are the top priorities laid out by Xi Jinping (Qingren 2014, p. 5). Restructuring the old Second Artillery Corps into the new Rocket Force elevated this branch of the army into a "separate" independent branch, with more autonomy, in decision-making. Furthermore, according to Stratfor, a private intelligence and analytical company based in Texas, another structure was created to support the military: ". . .the PLA Strategic Support Force's portfolio includes space, cyberspace and electronic warfare operations. . ..This lends credence to rumors that emerged as early as 2014 that the PLA was planning to establish a space force" (Stratfor 2016). Creating this branch in the military solely for space affairs underlines how aerospace and outer space are starting to be recognized as the next domain of congestion, competition, and contestation. In addition, China maintains a staggering defense spending budget of $151 billion US dollars (Global Security 2017). Ranking number two on the defense spending charts, China has increased steadily the PLA's budget in the last 20 years, every year by double digits (Stockholm International Peace Research Institute 2016). Despite trailing largely behind the USA in terms of defense expenditure, China shows clear commitment to developing a space defenses and a space capable force, to compete over the high ground. In the words of Tellis, "China simply cannot permit the creation of a space sanctuary because of its consequences for their own interest" (Tellis 2007, p. 50). If they allow the concept of sanctuary to be applied and space to remain free of weapons, surely all strategic advantages of outer space and a high ground will be lost and USA will remain a hegemon in space.

Chinese Space-Based Defense Technology

In line with the other three superpowers, technological determinism steers Beijing to develop new counterspace capabilities and acquire a strategic advantage. Chinese military scholars attitude towards future conflicts and their regard for outer space is found within the work of Chapman, referencing a quotation from Cpt. Shen Zongchang of the Chinese Naval Research Institute, "The mastery of outer space will be a requisite for military victory, with outer space becoming the new commanding heights for combat. . .lightning attacks and powerful first strikes will be more widely used in the future. . ..In future wars. . .radar, radio stations, communications facilities, and command ships [become] priority targets vulnerable to smart weapons, electronic attack, and electromagnetic pulse (EMP) weapons" (Chapman

2016, p. 73). Col. Bao Shixiu, professor in Military Affairs of the PLA, puts forward the rationale of how and why China will proceed with defensive weaponization of space, "An effective active defense against a formidable power in space may require China to have an asymmetric capability against the powerful United States. . ..an effective active defense strategy would include the development of these systems but would also include anti-satellite capabilities and space attack weapon systems if necessary. In essence, China will follow the same principles for space militarization and space weapons as it did with nuclear weapons. That is, it will develop anti-satellite and space weapons capable of effectively taking out an enemy's space system, in order to constitute a reliable and credible defense strategy" (Shixiu 2007, p. 9). Just like with Russia, deterrence is used as a defensive pretext, to develop defensive systems with offensive capabilities and discourage rivals from competing and contesting outer space. Also similar to Moscow, Beijing has begun emphasizing asymmetrical responses to the conventional US supremacy in the skies.

Satellites and Ground Infrastructure

"China's space industrial infrastructure is comprised of conglomerates of science and technology and R&D organizations. . .. . .This places a maximum premium on space-based sensors and other sensor platforms to facilitate surveillance, intelligence, and reconnaissance-related information pertaining to areas of national interest" (Khan and Khan 2015, p. 189). The following passage shows how in the modern age, satellite reliance on information, surveillance, and reconnaissance is crucial to maintaining a strategic advantage, when it comes to knowledge. China operates a large fleet of diverse satellites with various functions enabling them to meet the new security challenges. The satellite families can be categorized by four main functions: photographic reconnaissance, navigation, weather, and military communication satellites. Although the former three are designed and used mainly for civilian purposes, they could serve for military purposes as well (Poduval 2012, p. 91). Currently China has four launching sites active with the newest one, Wenchang, becoming operational last year. According to western scholars, the Wenchang launch facility will increase Beijing's capacity to deploy large space-based assets, such as the "Tiangong" Space Lab (David 2014). Finally, the equivalent to the Russian Akvarel program is the Chinese "C4I2SR" network (Command, Control, Communications, Computers, Intelligence, Information, Surveillance, and Reconnaissance). The complex network is upgraded constantly to optimize the command and control of all space assets and to integrate any new defense systems (Khan and Khan 2015, p. 189). Providing information about the ground infrastructure intends for the reader to understand how much emphasis is put into the various activities, which China conducts to support their space program.

ASAT Systems

According to Chapman ". . . Chinese leaders view ASAT and offensive counterspace systems as inevitable, while striving to acquire various foreign technologies that could be used to develop active ASAT capabilities" (Chapman 2016, p. 73). Recognizing the inescapability of weaponization and ASAT systems, Tellis writes in her

work "Drawing on China's indigenous military tradition, which emphasizes stealth, deception and indirect approaches to warfare, and opportunities offered by emerging technologies, which enable effective asymmetric strategies focused on attacking an adversary's weaknesses, the Chinese military has concentrated on developing a wide range of material and non-material capabilities that would make 'defeating the superior with the inferior' possible" (Tellis 2007, p. 48). Observing US usage of space as a strategic advantage since Desert Storm in 1991, Beijing concluded that asymmetric responses would be needed to contest Washington. Hence, "Chinese strategists concluded, therefore, that any effort to defeat the United States would require a riposte against its Achilles heel: its space-based capabilities and their organic ground installations" (Tellis 2007, p. 48). In 2006 and 2007, China showed the world their first space weapons: a laser one and a kinetic one. The first ASAT test in 2006 blinded a US satellite with a directed energy weapon for a period of time (Tellis 2007, p. 56). In the following year, Beijing destroyed one of their unused old meteorology satellite using an ASAT kinetic weapon (Poduval 2012, p. 96). In the words of Commander Poduval, "The ASAT test in 2007 and the dazzling of an American satellite by ground based laser in 2006 are only the small and visible attempts by China to target space based assets and inform the world of their growing capabilities" (Poduval 2012, p. 94). Besides the conventional development of ballistic ASAT systems by direct attack or ground attack, China has also concentrated on electronic weapons as well. With physical attacks on space assets impossible due to consequences of international retaliation, "denial of service" attacks are sought after, displaying the indigenous military approach (Tellis 2007, p. 58). Electronic attacks allow China to evade any possible confrontation in the international realm, simultaneously harming the capabilities of US communications. Moreover, "Electronic attack is a transitory yet potent form of 'mission kill' that Chinese military planners seem determined to exploit in instances where counterspace 'hard kill' capabilities appear disadvantageous or beyond reach" (Tellis 2007, p. 58). Chinese expansion of counterspace capabilities clearly demonstrates the technological determinism behind the realist notion of a new space race.

Implications

There are a couple of considerations to be made before moving to the last part, implications. Firstly for the sake of the length of the analysis, other actors with space programs, such as the EU, India, or Japan, have been ignored. Some of them have cooperative programs, while others are emerging as new space powers. Currently in a multipolar world, these actors play an important part in creating coalitions and balancing the power, between the three superpowers. However, due to their space program inferiority in comparison to the big three, they were disregarded from the study. Second, the commercial sector has also been overlooked, but has had a significant impact on the technological innovation. What's more, with the exception of China, most of the US and Russian military space technology used was produced by commercial enterprises, subcontracted by the governments. The free

market and the ingenuity of American companies essentially won the Cold War for the USA. However, we live almost 30 years after the collapse of the Soviet Block, and the evolving technology and expanding scientific knowledge allows once again Russia and China to begin contesting and competing for the high grounds, traditionally controlled by the USA. Columba Peoples writes "National space policies consistently emphasize international cooperation and the peaceful uses of outer space," but on the other hand that there is a "Growing focus within national policies on the security uses of outer space" (Peoples 2011, p. 83). The notion of securitization and technological determinism is the foremost reasons for new military space technology. George Sariak hypothesizes that what constitutes military space technology is vast and varied in nature, which makes it hard to uniformly categorize (Sariak 2017, p. 52). When, in 2001, the Bush administration withdrew from the ABMT, Russia realized they could not prevent the USA, from placing weapons in outer space for "defense" purposes (Shoumikhin 2002, p. 96). Using defense as a rationale for deploying space technology with counterspace capabilities is possible, as long as the technology does not fit the description of a weapon, under the international treaties signed. Besides securitization and determinism, Robert Lawson writes "The apparent reaction to these developments by Chinese and Indian officials underscored the risk that some space security actors were beginning to assume that space would inevitably become weaponized, and were thus beginning long-term planning on this assumption. This highlighted the potential for a negative action-reaction cycle similar to those which animated arms competitions during the Cold War" (Lawson 2004, p. 192). This action-reaction cycle depicts the deterrence theory of military space technology. Nevertheless Sariak writes "Unlike nuclear weapons, proffered by deterrence theory academics to have a stabilizing effect on international relations due to a doctrine of mutual assured destruction, space weapons are destabilizing. It is an important factor that "first-strike deterrence does not exist for space weapons"." (Sariak 2017, p. 59). Therefore, realist theorists, such as Anantatmula and Pavelec, have proponed the American initiation of weaponization of space "The development and deployment of these weapons is not only inevitable, but justifiable from both national and global security positions." He rationalizes "In the end, the United States is the only state that will be able to wield the power rationally and with the reasonable assurance that this power will be used judiciously for global security" (Pavelec 2012, p. 46). Such a viewpoint is surely subjective to Sterling Pavelec as an American scholar. While concurring to other realists such as Morgenthau, we can assume that either Russia or China will not act irrationally, but surely challenge the US hegemony in space through various methods. Each country has a motive for weaponizing space. The USA needs to protect their space assets, in order to maintain their hegemony and strategic advantage of the high ground. For China and Russia, the main motivation derives from denying the US this advantage and securing their own space presence and control. All the while the three countries promote cooperation and prohibition of space weaponization, scholars from all three have produced plenty of literature on ways to congesting, competing, and contesting outer space. This literature reinforces the idea that conflict for outer space is inevitable, especially given the comprehensiveness of the counterspace capabilities invented.

Conclusion

Russia, China, and the United States have acknowledged high ground and outer space as the key component to holding a strategic advantage in future conflicts. As discussed before, space has been already militarized since the 1950s, with the first satellites sent by USA and USSR. These satellites play vital role in US hegemony. Initiating the securitization and cyber defense of those space-based assets can transgress into weaponization. In the previous paragraphs, we have illustrated how the development of military space policy has become vital to protecting both national and economic interests in outer space. Moreover, each of the three superpowers has created a comprehensive space policy in regards to the challenges posed by the other adversaries. Likewise in the last 15 years, we have seen a rapid increase in experimentation and development of numerous of ASAT systems. The big three have put forward various types of ASAT systems, some of which have already been tested successfully. The array of symmetrical and asymmetrical counterspace capabilities includes: laser, electronic, kinetic, or ballistic ASATs. Such exotic "space defenses" pose a destabilizing effect to the balance of power. Concurring to the realist perspective deploying "cyber defenses" to ensure security will agonize the peaceful coexistence between the big three presently in outer space. These space defenses will resemble very much new space offences.

Space Defense directly relates to Cyber-Defense, as the new field of contestation and competition. Hence, Cyber-Defense is related directly to the Cyber-Development of a nation state. And Cyber-Development allows for the nation state as an entity to develop Cyber-Democracy. In the near future times, we shall see more of these three terms as humanity thrives upon the technology it has developed. How will the different actors in this Space Race react to one another depends upon their needs and desires towards space as a common good. If most of them are driven by idealistic intentions, Cyber-Democracy shall prevail within the outer space system and the Cyber-Development shall be prosperous for the whole of humanity. Cyber-Defenses will pose a challenge to the latter mentioned terms; however, it will be a necessary prerequisite if we encounter foreign alien species. Nevertheless under the realistic paradigm, the three big terms – Cyber-Democracy, Cyber-Development, and Cyber-Defense – will be contested by the biggest actors in outer space regardless, in which sphere of life.

Cross-References

- ▶ Academic Firm in Cyber-Development: The New Design and Redesign Proposition for Entrepreneurship in the Innovation-Driven Knowledge Economy
- ▶ Citizenship Education and New Media: Opportunities and Challenges
- ▶ Cyber-Democracy in the Middle East
- ▶ Epistemic Governance and Epistemic Innovation Policy in Higher Education for Cyber-Development

► Libya: Where Cyber-Democracy Reached Its Limits – How the Case of Libya Challenges the Idea of Cyber-Development
► Quadruple and Quintuple Helix Innovation Systems and Mode 3 Knowledge Production

References

Anantatmula, V. (2013). U.S. initiative to place weapons in space: The catalyst for a space-based arms race with China and Russia. *Astropolitics: The International Journal of Space Politics & Policy, 11*(3), 132–155.

Armstrong, D. (2014) American national security and the death of space sanctuary. Astropolitics: The International Journal of Space Politics & Policy, 12(1), 69–81.

ACA. (2017). U.S. nuclear modernization programs. Retrieved 19 Aug 2017 from https://www.armscontrol.org/factsheets/USNuclearModernization.

Chambers, M. (2007). Framing the problem: China's threat environment and international obligations. In R. Kamphausen & A. Scobell (Eds.), *Right sizing the People's Liberation Army: Exploring the contours of China's military* (pp. 9–10). Carlisle: Strategic Studies Institute.

Chapman, B. (2016). Chinese military space power: U.S. Department of Defense annual reports. *Astropolitics: The International Journal of Space Politics & Policy, 14*(1), 71–89.

Chunsi, W. (2008). China's outer space activities: Motivations, goals, and policy. *Strategic Analysis, 32*(4), 621–635.

David, L. (2014). China's new spaceport to launch country's largest rocket yet. Retrieved 16 Aug 2017 from https://www.space.com/25323-china-new-spaceport-rocket-launches.html.

Day, D. (2003). Intelligence space programs. In E. Sadeh (Ed.), *Space politics and policy: An evolutionary perspective* (pp. 371–389). New York: Springer Publishing Company.

DeBlois, B. (1998) Space sanctuary. A viable national strategy. *Aerospace Power Journal*, Winter, p. 41.

DeBlois, B. (2003) The advent of space weapons. *Astropolitics: The International Journal of Space Politics & Policy*, 1(1), 29–53.

Dolman, E. (2001). *Astropolitik – Classical geopolitics in the Space Age*. London: Frank Cass Publishers.

Federation of American Scientists [FAS]. (2006). *US national space policy*. Retrieved 18 Aug 2017 from https://fas.org/irp/offdocs/nspd/space.pdf.

Global Security. (2017). China defense spending. Retrieved 18 Aug 2017 from http://www.globalsecurity.org/military/world/china/budget.htm.

Goddard, B. (2010). Cold warriors say no nukes. *The Hill*. Retrieved 17 Aug 2017 from http://thehill.com/opinion/columnists/ben-goddard/78391-cold-warriors-say-no-nukes.

Hamilton, R. (1995). *Precision guided munitions and the new era of warfare*. Air Power Studies Centre, Royal Australian Air Force. Retrieved 17 Aug 2017 from https://fas.org/man/dod-101/sys/smart/docs/paper53.htm.

Hays, P. (2003). Space and the military. In E. Sadeh (Ed.), *Space politics and policy: An evolutionary perspective* (pp. 335–371). New York: Springer Publishing Company.

Hickman, J., & Dolman, E. (2002). Resurrecting the Space Age: A state-centered commentary on the outer space regime. *Comparative Strategy Journal, 21*(1), 1–20.

Hoefer, C. (2008). Causal determinism. Stanford Encyclopedia of Philosophy, Winter 2009 ed. Retrieved 19 Aug 2017 from https://plato.stanford.edu/archives/win2009/entries/determinism-causal/.

Honkova, J. (2013). The Russian Federation's approach to military space and its military space capabilities. Retrieved 9 Aug 2017 from http://marshall.org/wp-content/uploads/2013/11/Russian-Space-Nov-13.pdf.

International Institute for Strategic Studies [IISS]. (2014). Chapter five: Russia and Eurasia. *The Military Balance Journal, 114*(1), 161–200.

Ionin, A. (2006). Russia's space program in 2006: Some progress but no clear direction. In *Moscow defense brief* (pp. 2–6). Centre for Analysis of Strategies and Technologies, Moscow, Russia.

Khan, Z., & Khan, A. (2015). Chinese capabilities as a global space power. *Astropolitics: The International Journal of Space Politics & Policy, 13*(2–3), 185–204.

Kornukov, A. (2001). Apropos of the grown role of confrontation in the aerospace sphere and Air Force tasks in 21st-century military operations. *Military Thought Journal*. Retrieved 16 Aug 2017 from http://www.highbeam.com/doc/1G1-80321751.html.

Krebs, G. (2017). Military Spacecraft – USA, *USA military satellites*. Retrieved 18 Aug 2017 from http://space.skyrocket.de/directories/sat_mil_usa.htm.

Kremlin. (2012). *Meeting on the implementation of the state program of armaments in the field of nuclear deterrence*, translated from Russian. Retrieved 9 Aug 2017 from http://kremlin.ru/events/president/news/16058.

Lawson, R. (2004). The space security index. *Astropolitics: The International Journal of Space Politics & Policy, 2*(2), 175–199.

Lupton, D. (1998). On space warfare, A space power doctrine, Airpower research Institute , Air University Press, Retrieved on 15 Aug 2017 from http://www.dtic.mil/dtic/tr/fulltext/u2/a421942.pdf.

MacDonald, B. (2009). *Steps to strategic security and stability in space: A view from the United States, Disarmament forum 4* (p. 17). Geneva: United Nations Institute for Disarmament Research.

McCabe, T. (2016). The Russian perception of the NATO aerospace threat: Could it lead to preemption? Retrieved 14 Aug 2017 from https://www.thefreelibrary.com/The+Russian+perception+of+the+NATO+aerospace+threat%3a+could+it+lead+to...-a0463513904.

Mearsheimer, J. (2001). *The tragedy of great power politics* (pp. 2–3). New York: W. W. Norton.

Moltz, J. C. (2008). *The politics of space security: Strategic restraint and the pursuit of national interests* (pp. 23–28). Stanford: Stanford University Press.

Morgenthau, H. J. (1948). *Politics among nations: The struggle for power and peace*. New York: A. A. Knopf.

Mowthorpe, M. (2002). The Soviet-Russian approach to military space. *The Journal of Slavic Military Studies, 15*(3), 25–48.

OECD. (2014). *The space economy at a glance 2014* (p. 18). OECD Publishing. Retrieved 19 Aug 2017 from https://doi.org/10.1787/9789264217294-en.

Pavelec, S. M. (2012). The inevitability of the weaponization of space: Technological constructivism versus determinism. *Astropolitics: The International Journal of Space Politics & Policy, 10*(1), 39–48.

Peoples, C. (2008). Assuming the inevitable? Overcoming the inevitability of outer space weaponization and conflict. *Contemporary Security Policy Journal, 29*(3), 502–520.

Peoples, C. (2011). The securitization of outer space: Challenges for arms control. *Contemporary Security Policy Journal, 32*(1), 76–98.

Poduval, S. (2012). China's military space capabilities. *Maritime Affairs: Journal of the National Maritime Foundation of India, 7*(2), 85–101.

Podvig, P. (2004). *Russian military space capabilities*. Federation of American Scientists. Retrieved 16 Aug 2017 from https://fas.org/pubs/_docs/10072004164624.pdf.

Podvig, P. (2013). Another old anti-satellite system resurfaces. In *Russian strategic nuclear forces*. Retrieved 16 Aug 2017 from http://russianforces.org/blog/2013/01/another_old_anti-satellite_sys.shtml.

Pollpeter, K. (2005). The Chinese vision of space military operations. In J. Mulvenon & D. Finkelstein (Eds.), *China's revolution in doctrinal affairs: Emerging trends in the operational art of the Chinese People's Liberation Army* (pp. 329–369). Alexandria: The CNA Corporation.

Qingren, S. (2014). *China's military reform: Prospects and challenges*. Institute for Security and Development Policy. Retrieved 15 Aug 2017 from http://isdp.eu/content/uploads/publications/2014-shi-qingren-chinas-military-reform-prospects-and-challenges.pdf.

Russia Embassy UK. (2015). *The military doctrine of the Russian Federation*. Retrieved 8 Aug 2017 from https://rusemb.org.uk/press/2029.

Sadeh, E. (2003). *Space politics and policy: An evolutionary perspective* (pp. 317–393). Boston: Kluwer.

Sariak, G. (2017). Between a rocket and a hard place: Military space technology and stability in international relations. *Astropolitics: The International Journal of Space Politics & Policy, 15*(1), 51–64.

Schelling, T. (1966). *The diplomacy of violence* (pp. 1–34). New Haven: Yale University Press.

School of Russian and Asian Studies [SRAS]. (2010). The Military Doctrine of the Russian Federation approved by Russian Federation Presidential Edict on 5 February 2010. Retrieved 14 Aug 2017 from http://www.sras.org/military_doctrine_russian_federation_2010.

Shipping, T. (2008). From offensive to defensive realism: A social evolutionary interpretation of China's security strategy. In R. S. Ross & F. Zhu (Eds.), *China's ascent: Power, security, and the future of international politics* (pp. 153–156). Ithaca: Cornell University Press. Retrieved 16 Aug 2017 from http://www3.ntu.edu.sg/rsis/publications/SSIS/SSIS003.pdf.

Shixiu, B. (2007). Deterrence revisited: Outer space. *China Security, 3*(1, Winter), 9.

Shoumikhin, A. (2002). Russian perspectives on the military uses of outer space. *Astropolitics: The International Journal of Space Politics & Policy, 1*(3), 95–112.

Stockholm International Peace Research Institute (SIPRI). (2016). Military expenditure database. Retrieved 9 Aug 2017 from https://www.sipri.org/databases/milex.

Small Arms Defense Journal [SADJ]. (2016). The US Navy's Electric Weaponry, Vol. 7. Retrieved 19 Aug 2017 from http://www.sadefensejournal.com/wp/?p=3459.

SpaceToday. (2017). Space launch sites around the world. Retrieved 18 Aug 2017 from http://www.spacetoday.org/Rockets/Spaceports/LaunchSites.html#USA.

Spacy, W. (2010). Assessing the military utility of space-based weapons. *Astropolitics: The International Journal of Space Politics & Policy, 1*(3), 1–43.

Stratfor. (2016). China takes bold steps toward military reform. Retrieved 15 Aug 2017 from https://worldview.stratfor.com/analysis/china-takes-bold-steps-toward-military-reform.

Subcommittee on Strategic Forces. (2017). H.R. 2810FY18 National Defense Authorization Bill. Retrieved 18 Aug 2017 from http://docs.house.gov/meetings/AS/AS00/20170628/106123/BILLS-115HR2810ih-STR.pdf.

TASS. (2015). Russia developing system capable of 'switching off' foreign military satellites. Retrieved 14 Aug 2017 from http://tass.com/russia/803788.

TASS. (2016). Russian Armed Forces upgrade prioritized in 2017–2019 budget. Retrieved 9 Aug 2017 from http://tass.com/economy/909427.

Tellis, A. J. (2007). China's military space strategy. *Survival Journal, 49*(3), 41–72.

Tellis, A. J. (2008). China's space capabilities and their impact on U.S. National Security (p. 2). Retrieved 19 Aug 2017 from http://carnegieendowment.org/files/AshleyJTellisUSCCTestimonyMay2020082.pdf.

U.S. Air Force [AF]. (2015). X-37B orbital test vehicle. Retrieved 19 Aug 2017 from http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104539/x-37b-orbital-test-vehicle/.

U.S. Department of Defense [DOD]. (2000). *Report to Congress pursuant to the FY 2000 National Defense Authorization Act: Annual report on the military power of the People's Republic of China* (p. 14). Washington, DC: Government Publishing Office. Retrieved 19 Aug 2017 from http://purl.access.gpo.gov/GPO/LPS24358.

U.S.DOD. (2011). *National security space strategy*. Federation of American Scientists. Retrieved 18 Aug 2017 from https://fas.org/irp/eprint/nsss.pdf.

U.S.DOD. (2016). Releases fiscal year 2017 president's budget. Retrieved 18 Aug 2017 from https://www.defense.gov/News/News-Releases/News-Release-View/Article/652687/department-of-defense-dod-releases-fiscal-year-2017-presidents-budget-proposal/.

Union of Concerned Scientists [UCS]. (2017). UCS Satellite Database. Retrieved 26 Aug 2017 from http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.WZmztz4jHct.

Vorobyov, I., & Kiselyov, V. (2007). The promise of defense. *Military Thought Journal*. Retrieved 14 Aug 2017 from http://www.highbeam.com/doc/1G1-166433360.html.

Waltz, K. N. (1979). *Theory of international politics* (p. 10). Reading: Addison-Wesley.

Webb, D. (2015). The ethical use of outer space. In M. Hersh (Ed.), *Ethical engineering for international development and environmental sustainability* (p. 112). London: Springer.

Wolff, J. (2003). *Peaceful use' of outer space has permitted its militarization – Does it also mean its weaponization? Disarmament forum 1* (pp. 5–13). Geneva: United Nations Institute for Disarmament Research.

Part II

Cyber-Democracy

Overview of Cyber-Democracy

17

David F. J. Campbell and Elias G. Carayannis

Advanced democracies or democracies of a high quality are also a "knowledge democracy." One underlying understanding here is that knowledge, knowledge creation, knowledge production, and knowledge application (innovation) behave as crucial drivers for enhancing democracy, society, and the economy. Knowledge democracy fosters and excels innovation, and the interplay of knowledge and innovation enables, supports, and carries sustainable development. Between political pluralism in democracy and the diversity and heterogeneity of knowledge in a knowledge society and knowledge economy, there operates a congruence in structures and processes. Knowledge democracy does not only apply to industrialized countries but offers, in principle, also important references for developing democracies, the newly industrialized countries and the emerging (and developing) markets. The implication of "cyber-democracy" is to look at knowledge democracy from the perspective of a globally evolving knowledge society in configurations of a multilevel architecture (global, transnational, supranational, national, subnational, and local). Ramifications of cyber-democracy are: (1) the

D. F. J. Campbell (✉)
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@donau-uni.ac.at

E. G. Carayannis
Department of Information Systems and Technology Management, School of Business, The George Washington University, Washington, DC, USA
e-mail: caraye@gwu.edu

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_72

networking opportunities and capabilities of interaction and communication increase; (2) the volume of codified knowledge cumulates, and the possibilities to access (publicly access) this knowledge also improve; (3) digitalized (electronic) information and knowledge, and the World Wide Web, created a network-style fundament and infrastructure of knowledge, allowing a knowledge conversion of the local into the global (*gloCal*) and vice versa, resulting in a *gloCal* platform for communication and knowledge interaction and knowledge enhancement. How does cyber-democracy relate to cyber-development and cyber-defense? Cyber-democracy raises challenges for governance and of governance and the next steps of further development of society and democracy.

Propositions for further discussions are:

1. *Cyber-Democracy and Knowledge Democracy:* The progress of advanced economies and of quality of democracy depends on knowledge economy, knowledge society, and knowledge democracy, their co-evolution and their mutual interlinkages (Carayannis and Campbell 2009, 2010, 2012; Campbell and Carayannis 2013). The transformation and shift has been from a knowledge-based economy and society directly to a knowledge economy and knowledge society. Pluralism and heterogeneity are crucial and decisive for progressing quality of democracy. The analogy to knowledge is that advanced knowledge systems are also characterized by a pluralism, diversity, and heterogeneity of different knowledge paradigms and innovation paradigms (and modes of knowledge production) that drive in co-evolution the interaction and relationship of competition, cooperation, and learning processes. *Cyber-democracy, in fact, amplifies and accelerates the momentum of knowledge democracy. Cyber-democracy is connected to democracy by building and by forming IT-based infrastructures and public spaces, where IT (information technology) helps in creating new types and new qualities of public space*. The concept and model of the "Quadruple Helix Innovation System" (Carayannis and Campbell 2009, 2012) explicitly identifies the "media-based and culture-based public" (in addition to "civil society") as the one crucial helix or context for carrying on and advancing knowledge production and innovation. Therefore, in these aspects, the cyber-democracy and knowledge democracy overlap in a conceptual understanding, but also in the manifestation of empirical phenomena. Cyber-democracy expresses a particular vision, for how knowledge democracy may evolve further in certain and particular characteristics. *IT-based public spaces in Cyber-democracy operate nationally and subnationally. Cyber-democracy, however, also transcends the boundaries of the nation state, as such adding to the building of a transnational, in fact global public space.* Public spaces in cyber-democracy are certainly multilevel (global, national, and subnational). The global and transnational aspect of public space in cyber-democracy certainly represents this one very new and radical aspect, allowing for a global spreading of knowledge and of high-quality knowledge, in this case enabling continuous flows of knowledge and discourses beyond the limits of the nation state.

2. *Cyber-Democracy and Governance:* Cyber-democracy appears to have several implications for governance of democracy and governance in democracy. In an etymological understanding, the origin of the word "governance" refers back to ancient Greek (the verb *kybernein* or κυβερνειν infinitive, *kybernao* or κυβερνάω first person), where the literal meaning was to steer or to guide a vehicle that was land-based or sea-based (a ship), but Plato already emphasized the idea of governance of men or of people. The prefix "cyber" thus explicitly reflects the etymological component of "steering" (Campbell and Carayannis 2013, p. 3). Based on this assignment, we could paraphrase "cybernetics" as a science of steering. Cybernetics refers to feedback and focuses on regulatory systems, but of course there exist different approaches to cybernetics (Wiener 1948; Umpleby 1990). *Cyberdemocracy, therefore, may be understood as a governance of democracy in context of knowledge democracy. This governance can be interested and motivated to use (also to use) new IT-based infrastructures (for example the internet or web) and public spaces for purposes of governance. Furthermore, public spaces (advanced public spaces) also define references for quality of governance in democracy. We can speculate, how these public spaces also may have references and ramifications for "media-based and culture-based public" that is being identified by the model of the "Quadruple Helix Innovation System" as being crucial for knowledge production and the progress of innovation* (Carayannis and Campbell 2009, 2012).
3. *Cyber-Democracy, Global Democracy and Global Society:* The concept of "global democracy" can take different meanings. Global democracy could be translated into regimes and systems of intergovernmental cooperation or supranational integration (e.g., in context of the European Union). This implies to tie global democracy directly to mechanisms of government and governance. Alternatively, we may want to think of global democracy more in terms of an evolving (self-evolving) of a *global society. Particularly the features of an international knowledge flow and of IT-based infrastructures (and of public spaces), which clearly transcend the borders and boundaries of nation states, support the notions of a global society, where, at least partially, the global society even bypasses the nation state*. In that scenario, the global society would develop vis-à-vis the traditional nation state. One consequence of this is that nation states do not have the power anymore of controlling or suppressing successfully the global flow of knowledge. The spreading of political unrest and of growing demands for more democracy in context of authoritarian or semi-authoritarian regimes during the recent phase of the "Arab Spring" represents here a perfect example for these new political phenomena. But of course, also the concept of *global society* would have to be translated into a multilevel architecture of arrangements, distinguishing between global, national and subnational levels within context of the *global society* (global knowledge society).
4. *Cyber-Democracy and the New Rights and New Freedoms:* Cyber-democracy provides governments in democracies (and in non-democracies) with additional IT-based technical means and capabilities of monitoring the flow of knowledge on the internet. *But of course, not everything, which is technically possible, is also*

feasible in terms of democracy and quality of democracy. This creates a need for restricting (technically possible) monitoring activities of democratic governments against their own citizens and residents. Democratic governments, in fact, should impose on themselves also self-restrictions in that respect. Where is here the line to be drawn? For example: Does an e-mail qualify, in a legal sense, as a "postcard" or as a "letter"? Letters demand a higher protection standard. *It is obvious that cyber-democracy requires a debate and discourse on the new rights and new freedoms of citizens in context of knowledge democracy, protecting citizens against monitoring activities of their governments that are at conflict with principles of quality of democracy.* This also refers to the relationship and interaction activities of governments in the international system. For example, a new standard to-be-discussed could be that governments of democratic countries (who are also allies in the international arena) do not "spy" against each other. "No-spy" activities would imply that democratic governments respect mutually (at least in principle) the quality of their democratic regimes and democratic systems. Continued "spying," on the other hand, would create problems for the building of trust and respect among democratic governments.

References

Campbell, D. F. J., & Carayannis, E. G. (2013). *Epistemic governance in higher education. Quality enhancement of universities for development* (SpringerBriefs in business). New York: Springer. http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6.

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "Quadruple helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46* (3/4), 201–234. http://www.inderscience.com/browse/index.php?journalID=27&year=2009&vol=46&issue=3/4 and http://www.inderscience.com/search/index.php?action=record&rec_id=23374&prevQuery=&ps=10&m=or.

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69. http://www.igi-global.com/bookstore/article.aspx?titleid=41959.

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development* (SpringerBriefs in business, Vol. 7). New York: Springer. http://www.springer.com/business+%26+management/book/978-1-4614-2061-3 and http://www.springer.com/cda/content/document/cda_downloaddocument/9781461420613-c1.pdf?SGWID=0-0-45-1263639-p174250662.

Umpleby, S. A. (1990). The science of cybernetics and the cybernetics of science. *Cybernetics and Systems, 21*(1), 109–121. ftp://ftp.vub.ac.be/pub/projects/Principia_Cybernetica/Papers_Umpleby/Science-Cybernetics.txt.

Wiener, N. (1948). *Cybernetics or control and communication in the animal and the machine*. New York: Wiley.

Quality of Democracy in Quadruple Helix Structures: OECD Countries in Global Comparison

18

David F. J. Campbell and Elias G. Carayannis

Contents

D. F. J. Campbell (✉)
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@univie.ac.at; david.campbell@uni-ak.ac.at; david.campbell@aau.at

E. G. Carayannis
Department of Information Systems and Technology Management, School of Business, The George Washington University, Washington, DC, USA
e-mail: caraye@gwu.edu

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_7

Abstract

The analytical research question of this chapter is threefold: (1) To develop (and to prototype) a conceptual framework of analysis for a global comparison of quality of democracy. This framework also references to the concept of the "Quadruple Helix innovation systems" (created by Carayannis and Campbell and first published in 2009). (2) The same conceptual framework is being used and tested for comparing and measuring empirically quality of democracy in the different OECD and European Union (EU27) member countries. (3) Finally (and based on the international comparison), different propositions and recommendations for an improvement of quality of democracy reform in Austria are being developed and suggested. By this, Austrian democracy qualifies as a case study for democracy enhancement. In theoretical and conceptual terms, we refer to a Quadruple-dimensional structure, also a Quadruple Helix structure (a "Model of Quadruple Helix Structures") of the four basic (conceptual) dimensions of freedom, equality, control, and sustainable development for explaining and comparing democracy and quality of democracy. Put in summary, we may conclude for the United States: the comparative strength of quality of democracy in the United States focuses on the dimension of freedom. The comparative weakness of the quality of democracy in the United States lies in the dimension of equality, most importantly income equality. Quadruple Helix refers here to at least two crucial perspectives: (1) the unfolding of an innovative knowledge economy also requires (at least in a longer perspective) the unfolding of a knowledge democracy and (2) knowledge and innovation are being defined as key for sustainable development and for the further evolution of quality of democracy. How to innovate (and reinvent) knowledge democracy? There is a potential that democracy discourses and innovation discourses advance in a next-step and two-way mutual cross-reference. The architectures of Quadruple Helix (and Quintuple Helix) innovation systems demand and require the formation of a democracy, implicating that quality of democracy provides for a support and encouragement of innovation and innovation systems, so that quality of democracy and progress of innovation mutually "Cross Helix" in a connecting and amplifying mode and manner. This relates research on quality of democracy to research on innovation (innovation systems) and the knowledge economy. "Cyber-democracy" receives here a new and important meaning.

Keywords

Austria · Basic Quadruple-dimensional structure of quality of democracy · Cyber-democracy · Democracy · Democracy improvement and reform · Equality · Freedom · Interdisciplinary · International comparison of OECD and European Union member countries · Knowledge democracy · Quadruple and Quintuple Helix · Quadruple Helix innovation systems · Quality of democracy · Sustainable development · Transdisciplinary · United States

Introduction: Research Design and Research Question for the Comparative Analysis

This chapter focuses on analyzing quality of democracy in a comparative approach. Even though comparisons are not the only possible or legitimate method of research, our contribution is based on the opinion that comparisons provide crucial analytical perspectives and learning opportunities. Therefore, our analysis is being guided and governed by the following proposition: *national political systems (political systems) are comprehensively understood only by using an international comparative approach.* International comparisons (of country-based systems) are common (see the status of comparative politics, e.g., in Sodaro 2004). Comparisons do not have to be based necessarily on national systems alone but can also be carried out using "within" comparisons inside (or beyond) subunits or regional subnational systems, for instance, the individual provinces in the case of Austria (Campbell 2007, p. 382).

The pivotal analytical research question of this chapter is threefold:

1. To develop (to "prototype") a conceptual framework of analysis for a global comparison of quality of democracy. This framework will also reference to the concept of the "Quadruple Helix innovation systems" (Carayannis and Campbell 2009, 2014, 2015). Quadruple Helix and Quadruple Helix structures represent here an interdisciplinary (and transdisciplinary) linkage that connects research in quality of democracy with innovation concepts (see also Bast et al. 2015; furthermore, see also the website of "Arts, Research, Innovation and Society," ARIS: http://www.dieangewandte.at/aris). This interdisciplinary perspective should furthermore emphasize the overall importance of knowledge (and of knowledge and innovation) for society, economy, and democracy.
2. This same conceptual framework will be used and will be tested for comparing and measuring quality of democracy in the different OECD and European Union (EU27) countries. First propositions are being formulated about democracy in the United States but clearly need further follow-up inquiry in a later phase and discourse. This comparison is more exploratory in nature and character and wants to provide further evidence about the usefulness of the developed framework. This framework should inspire and inform future research on quality of democracy but also future research in reference to knowledge and innovation systems (see also Campbell 2012; Campbell et al. 2013, 2015; Campbell and Carayannis 2014).
3. Finally (and based on the international comparison), different propositions and recommendations for an improvement of quality of democracy reform in Austria are being developed and suggested: by this, Austrian democracy qualifies as a case study for democracy enhancement (see also Campbell 2015a, b; Campbell and Carayannis 2014).

In our analysis presented here, quality of democracy should be compared mutually between all member countries to the OECD (Organization for Economic

Cooperation and Development) and all the member countries to the European Union (EU15, EU27, without Croatia), thus leading to a country-based comparison of democratic quality (most, however not all member countries of the EU are also member countries to the OECD). Supranational aggregations (like of the whole European Union at the EU level of institutions) or transnational aggregations (global level) shall not be dealt with. The OECD consists primarily of the systems of Western Europe (EU as well as non-EU), North America (United States and Canada), Japan, Australia, and New Zealand. Outside these regions, Israel, Mexico, and Chile are part of the OECD, which highlights the global expansion and reach of OECD. The OECD countries can be *majorly* determined over the following two features: economically as "advanced economies" (IMF 2011, p. 150) and politically the majority of the OECD countries are determined as "established democracies" or as "Western democracies." Furthermore, we may also discuss, how relevant the concepts of "advanced societies" and "advanced democracies" are (Carayannis and Campbell 2011, p. 367; also 2012). However, in this context it appears more crucial that the OECD countries (again by the majority) can be seen as an empirical manifestation of liberal democracy, as known in the beginning of the twenty-first century. Ludger Helms (2007 p. 18) pointed out: "For a system to be identified as a liberal democracy, or simply as liberal-democratic, liberal as well as democratic elements have to be realized in adequate volumes" (quotes from original sources in German were translated into English by the authors of this analysis). Just as decisive is Helms' (2007 p. 20) statement: "The political systems of Western Europe, North America and Japan examined in this study can be distinguished – despite all the differences – as liberal democracies." Since the OECD countries are majorly represented by advanced democracies and advanced economies, the OECD countries are very suitable as a peer group for the comparisons of different OECD countries, for example, the United States with other OECD countries, in order to carry out a "fair" comparison. For a comparison of the quality of democracy of the United States with other countries (democracies), the "comparative benchmark" must be of the highest possible standard, in order to submit propositions that test the actual quality of a concrete democracy. *Concerning quality of democracy, what can the United States learn from other democracies?* This same question applies also to all the other democracies.

This emphasis of the OECD comparative assessment of quality of democracy will not be based on a time series pattern; instead (see section "The International Comparison (Part One): Focus on the Year 2010"), it will focus on an indicator-specific system using empirical information available from a more recent year (mostly 2010, referring to data publicly accessible as of early 2012). Since our analysis is more explorative in character (wanting to test the design of a developed comparative framework), the year 2010 qualifies as sufficiently recent. However, in section "The International Comparison (Part Two): Comparison of the Years 2011–2012 and 2014–2015," also a trend comparison of the years 2011–2012 and 2014–2015 is being presented additionally, with a discussion of the results. The mentioned reference year of 2010 or 2012 explains why we did not include Croatia into our analysis. Croatia joined the European Union as late as 2013, creating by this

the EU28. With the planned retreat of the United Kingdom (UK) from the EU, as a consequence of the British "Brexit" referendum in 2016, the EU then would transform back into an EU27. The UK withdrawal from EU is expected to take place during the course of the year 2019. To support our analysis, a broad spectrum of indicators will be considered for this purpose of comparative inquiry, which appears to be necessary in order to conclude different (underlying) theories and models about quality of democracy. Follow-up studies will certainly be conceivable to integrate this empirically comparative snapshot of the quality of democracy. As of August 2017, the OECD has 35 member countries (http://www.oecd.org/about/membersandpartners/). *These OECD member countries define the primary reference framework for the international comparison in this analysis*. Since not every member state of the current EU27 is a member of the OECD, the decision to include the non-OECD countries of the EU27 countries was made for the country comparison, which therefore results in an expansion of the group of countries to "OECD plus EU27." These additional countries are Bulgaria, Latvia, Lithuania, Malta, Romania, and Cyprus. In total, our presented country sample for the comparison of quality of democracy consists of about 40 countries.

There is naturally not only a single democracy theory (theory about quality of democracy), but the field of democratic theories is rather pluralistic and heterogeneous. Various theories and models coexist about democracies (Cunningham 2002; Held 2006; Munck 2014; Schmidt 2010). Metaphorically, based on these (partly contradictory) different theories, democracy theory could also be constructed as a *metatheory*. Theoretically, democracy can be understood as *multi-paradigmatic*, meaning that there is not only one (dominant) paradigm for democracy. Therefore, we have to state pluralism, competition, coexistence and co-development of different theories about democracy. *Our analysis is based on the additional assumption (which does not have to be shared necessarily) that between democracy theory on the one hand and democracy measurement on the other hand, important (also conceptual) cross-references (and linkages) take place. Within this logic, a further development or improvement of the democracy theory demands a systematic attempt of democracy measurement, regardless of how incomplete or problematic an empirical assessment of democracy is*. Just like there is no "perfect" democracy measurement, there is also no "perfect" democracy theory (see, e.g., Campbell and Barth 2009; Geissel et al. 2016; Helms 2016; Lauth et al. 2000; Lauth 2004, 2010, 2011, 2016; Munck 2009, 2014; Schmidt 2010, pp. 370–398). Theories about the quality of democracy are partly already further developed, than it is often (in popular research) being assumed. One of the most important theory models about the quality of democracy that permits an empirical operationalization comes from Guillermo O'Donnell (2004a, b). The field of the quality of democracy is no longer a vague one, especially not for OECD countries.

The further structure of this chapter is divided into the following sections: in section "Conceptualizing Democracy and the Quality of Democracy: Freedom, Equality, Control and Sustainable Development (Model of Quadruple Helix Structures)," different conceptualizations of democracy and of quality of democracy are being presented, followed (in section "The Quality of Democracy in Comparative

Perspective: A Comparative Empirical View of the OECD Countries (and EU27 Member Countries) Relating to the Dimensions of Freedom, Equality, Control, and Sustainable Development") by the concrete empirical comparison of quality of democracy in the OECD countries and the member countries to the European Union. In the conclusion (section "Conclusion: Quality of Democracy in Quadruple Helix Structures"), we attempt to assess quality of democracy in the United States, based on the formulation of first propositions, and furthermore engage in propositions and recommendations for a further quality of democracy reform in Austria. In the epilogue (section "Epilogue on Cyber-Democracy"), we develop and discuss further moving thoughts on cyber-democracy. Furthermore, the "Quadruple Helix" is being emphasized as an interdisciplinary and a transdisciplinary approach for bringing democracy discourses and innovation discourses closer together.

Conceptualizing Democracy and the Quality of Democracy: Freedom, Equality, Control, and Sustainable Development (Model of Quadruple Helix Structures)

How can democracy and the quality of democracy be conceptualized? Such a (theoretically justified) conceptualization is necessary in order for democracy and the quality of democracy to be subjected to a democracy measurement, *whereby democracy measurement, in this case, can be examined along the lines of the definition of democracy (thus democracy measurement to be utilized to improve the democracy theory).* Hans-Joachim Lauth (2004, pp. 32–101) suggests in this context a "three-dimensional concept of democracy," which is composed of the following (conceptual) dimensions: *equality*, *freedom*, *and control* (see Figs. 1 and 2). *These dimensions we want to interpret as "basic dimensions" of democracy and of the quality of democracy.* Lauth (2004, p. 96) underlines that these dimensions are "sufficient" to obtain a definition of democracy. The term "dimension" offers a conceptual elegance that can be applied "trans-theoretically," meaning that different theories of democracy may be put in relation and may be mapped comparatively in reference to those dimensions. Metaphorically formulated, dimensions behave like "building blocks" for theories and the continuing development of theory. In the following analysis (see later), we furthermore propose to introduce "sustainable development" as a further basic dimension for democracy and quality of democracy. *To do this was (first) explicitly suggested by Campbell* (2012, pp. 296, 301–302; see also Campbell 2017).

Empirically, it should also be added that the traditional public perception of Western Europe indicates that individuals with a more-left political orientation prefer equality and individuals with a more-right (conservative) political orientation have preferences for freedom (Harding et al. 1986, p. 87). The European left/right axis would translate itself well for the North American contexts by using a liberal/conservative axis (with left = liberal and right = conservative).

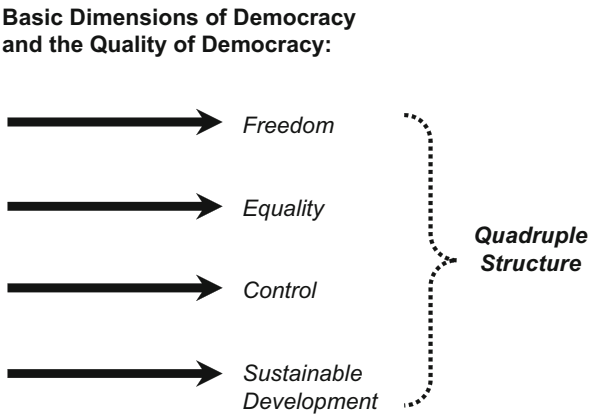


Fig. 1 The basic Quadruple-dimensional structure of democracy and the quality of democracy (Source: Authors' own conceptualization and visualization based on Campbell (2008, p. 32; 2012, p. 296), Campbell and Carayannis (2013a), and for the dimension of "control" on Lauth (2004, pp. 32–101))

With regard to democracy and the quality of democracy, we are confronted with the following point-of-departure question: whether (1) democracy as a key feature or criterion exclusively refers or should refer to the political system or whether (2) democracy should also include social (societal), economic, as well as ecological contexts of the political system. This produces implications on the selection of indicators to be used for democracy measurement. How "limited" or "broadly" focused should be the definition of democracy? This is also reflected in the *minimalistic* versus *maximalist* democracy theory debate (see, e.g., Sodaro 2004, pp. 168, 180, and 182). In this regard, various theoretical positions elaborate on this concept. Perhaps, it is (was) from an orthodox point of view of theory to limit democracy to the political system (Munck 2009, pp. 126–127). More recent approaches are more sensitive for the contexts of the political system, however, still must establish themselves in the political mainstream debates (see, e.g., Stoiber 2011). Nevertheless, explicit theoretical examples are emerging for the purpose of incorporation into the democracy models the social (societal), economic, and ecological contexts. The theoretical model of the "Democracy Ranking" is an initiative that represents such an explicit example (Campbell 2008; Campbell et al. 2013). The Democracy Ranking is an international civil society initiative that measures regularly quality of democracy in a global approach and comparison (for more detailed information, visit the website of the Democracy Ranking at: http://democracyranking.org/).

Over time, democracy theories are becoming more complex and demanding in nature, regardless, whether the understanding of democracy refers only to the political system or includes also the contexts of the political system. This also reflects on the establishment of democracy models or models of politics (see here, for an overview: Campbell 2013; Geissel et al. 2016; Giebler and Merkel 2016; Helms 2016; Lauth 2016; Morlino and Quaranta 2016; Munck 2014; Schedler 2006; Schmitter 2004). The most simple democracy model is that of the "electoral democracy" (Helms 2007, p. 19), also known as "voting democracy" ("*Wahldemokratie*"; Campbell and Barth 2009, p. 212). An electoral democracy focuses on the process of

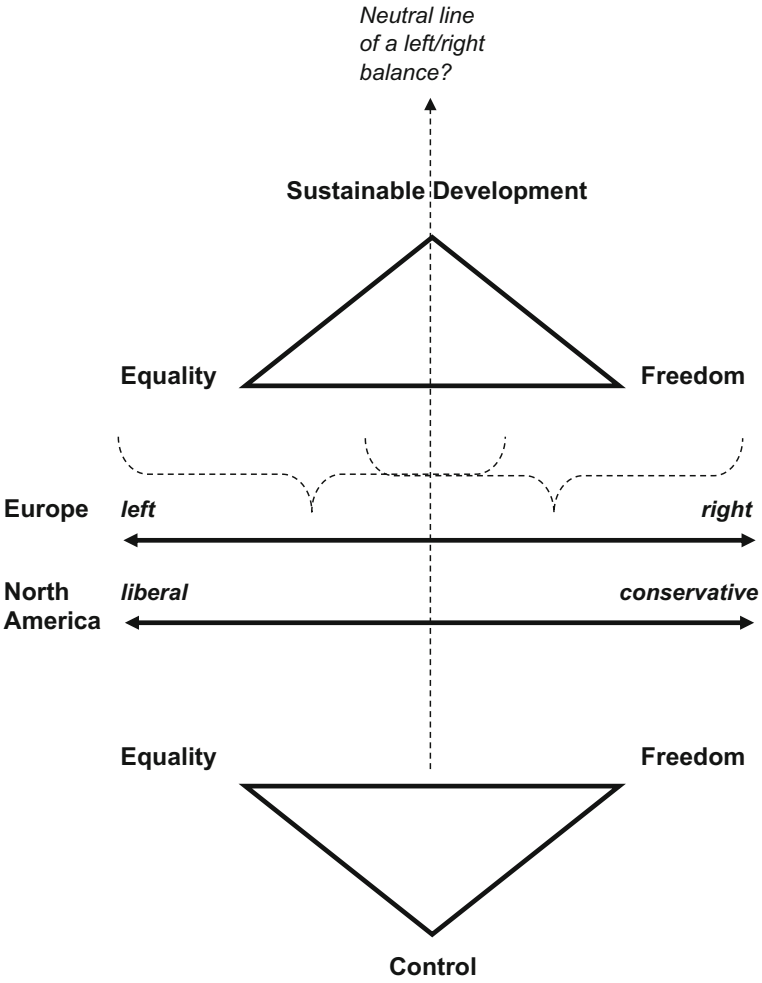


Fig. 2 Dimensions (conceptual dimensions) for the measurement of democracy and the quality of democracy (Source: Authors' own conceptualization and visualization based on Campbell (2008, p. 32; 2012, p. 296) and (for the lower triangle) on Lauth (2004, pp. 32–101))

elections, highlights the political rights, and refers to providing minimum standards and rights, however, enough to be classified as a democracy. Freedom House (2011a) defines electoral democracy by using the following criteria: "A competitive, multi-party political system," "Universal adult suffrage for all citizens," "Regularly contested elections," and "Significant public access of major political parties to the electorate through the media and through generally open political campaigning." The next, qualitatively better level of democracy is the so-called liberal democracy. A liberal democracy is characterized by political rights and more importantly also by civil liberties as well as complex and sophisticated forms of institutionalization. The

liberal democracy does not only want to fulfill minimum standards (thresholds) but aims on ascending to the quality and standards of a developed, hence, an advanced democracy. Every liberal democracy is also an electoral democracy, but not every electoral democracy is automatically a liberal democracy (on elections see also Rosenberger and Seeber 2008). In this regard, Freedom House (2011a) states: "Freedom House's term 'electoral democracy' differs from 'liberal democracy' in that the latter also implies the presence of a substantial array of civil liberties. In the survey, all the 'Free' countries qualify as both electoral and liberal democracies. By contrast, some 'Partly Free' countries qualify as electoral, but not liberal, democracies." Asserting different (perhaps ideal-typical) conceptual stages of development for a further quality increasing and progressing of democracy, we may put up for discussion the following stages: *electoral democracy*, *liberal democracy*, and *advanced (liberal) democracy* with a *high quality of democracy.*

In *Polyarchy*, Robert A. Dahl (1971 pp. 2–9) comes to the conclusion that mostly two dimensions suffice in order to be able to describe the functions of democratic regimes: (1) *contestation* ("public contestation," "political competition") as well as (2) *participation* ("participation," "inclusiveness," "right to participate in elections and office"). In Figs. 3 and 4, we propose to interpret these two dimensions, introduced by Dahl, as "secondary dimensions" for describing democracy and democracy quality for the objective of measuring democracy. Also relevant are Anthony Downs' eight criteria in *An Economic Theory of Democracy* (1957, pp. 23–24), defining a "democratic government," but it could be argued that those are affiliated closer with an electoral democracy. In the beginning of the twenty-first century is the conceptual understanding of democracy and the quality of democracy already more differentiated, it can be said that crucial conceptual further developments are in progress. Larry Diamond and Leonardo Morlino (2004, pp. 22–28) have come up with an "eight dimensions of democratic quality" proposal. These include (1) *rule of law*, (2) *participation*, (3) *competition*, (4) *vertical accountability*, (5) *horizontal accountability*, (6) *freedom*, (7) *equality*, and (8) *responsiveness*. Diamond and Morlino (2004, p. 22) further state: "The multidimensional nature of our framework, and of the growing number of democracy assessments that are being conducted, implies a pluralist notion of democratic quality." These eight dimensions distinguish themselves conceptually with regard to procedure, content, as well as results as the basis (conceptual quality basis) to be used in differentiating the quality of democracy (see Diamond and Morlino 2004, pp. 21–22; 2005; see also Campbell and Barth 2009, pp. 212–213). The "eight dimensions" of Diamond and Morlino may be interpreted as "secondary dimensions" of democracy and the quality of democracy for the purpose of democracy measurement (see again Figs. 3 and 4).

"Earlier debates were strongly influenced by a dichotomous understanding that democracies stood in contrast to non-democracies" (Campbell and Barth 2009, p. 210). However, with the quantitative expansion and spreading of democratic regimes, it is more important to differentiate between the qualities of different democracies. According to Freedom House (2011b), in the year 1980, no less than 42.5% of the world population lived in "not free" political contexts. By 2010, this share dropped to 35.4%. Democracies themselves are subject to further

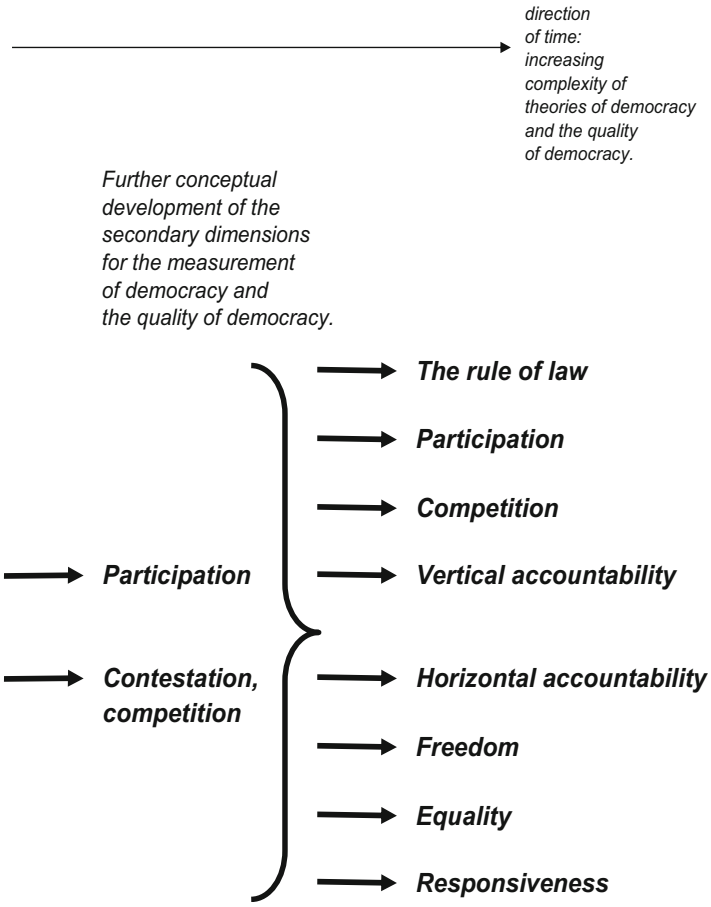


Fig. 3 Dimensions (secondary dimensions) for the measurement of democracy and the quality of democracy (Part A) (Source: Authors' own conceptualization and visualization based on Dahl (1971), Diamond and Morlino (2004, pp. 20–31; 2005), and Campbell (2008, p. 26))

development, which is a continuous process and does not finish upon its establishment. Democracies have to find answers and solutions to new challenges and possible problems. Democracies are in constant need to find and reinvent themselves. Observed over time, different scenarios could take place and could keep a democracy quality going on constantly; democracy quality could erode but also improve. *A betterment of the quality of democracy should be the ultimate aim of a democracy. Earlier ideas about an electoral democracy are becoming outdated and will not suffice in today's era.*

Guillermo O'Donnell (2004a) developed a broad theoretical understanding of democracy and the quality of democracy. In his theoretical approach, quality of democracy develops itself further through an interaction between human development and human rights: "True, in its origin the concept of human development

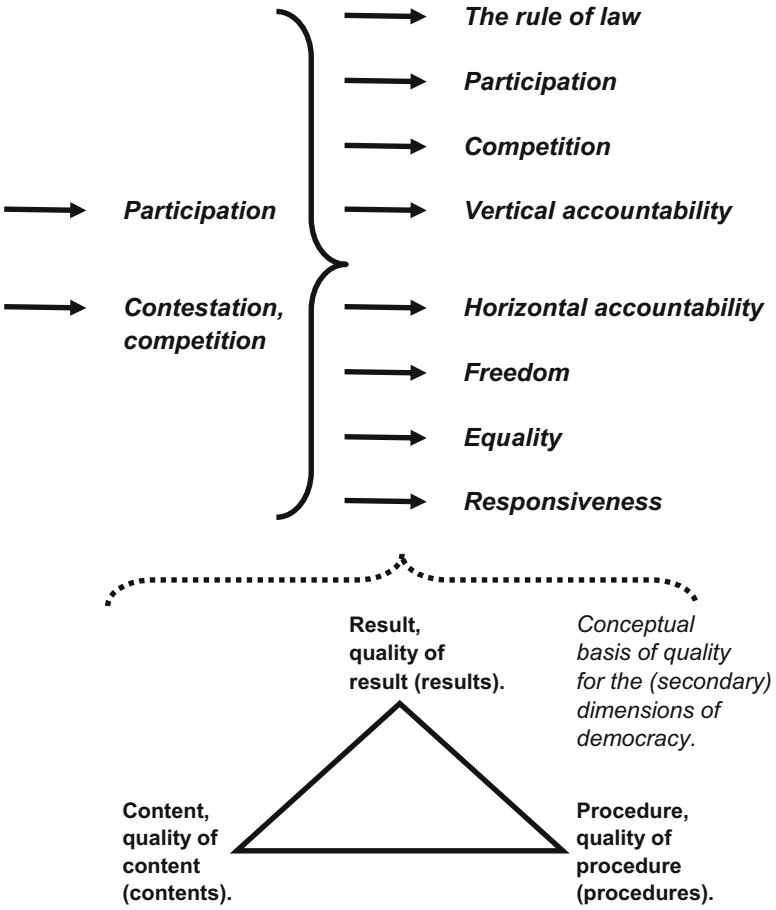


Fig. 4 Dimensions (secondary dimensions) for the measurement of democracy and the quality of democracy (Part B) (Source: Authors' own conceptualization and visualization based on Dahl (1971), Diamond and Morlino (2004, pp. 20–31; 2005), and Campbell (2008, p. 26))

focused mostly on the social and economic context, while the concept of human rights focused mostly on the legal system and on the prevention and redress of state violence" (O'Donnell 2004a, p. 12). The human rights differentiate themselves in civil rights, political rights, and social rights, in which O'Donnell (2004a, p. 47) assumes and adopts the classification of T. H. Marshall (1964). Human development prompts ". . .what may be, at least, a minimum set of conditions, or capabilities, that enable human beings to function in ways appropriate to their condition as such beings" (O'Donnell 2004a, p. 12), therefore in accordance with human dignity and, moreover, the possibility of participating realistically in political processes within a democracy. O'Donnell also refers directly to the *Human Development Reports* with the *Human Development Index (HDI)* that are being released and published annually

by the United Nations Development Program (UNDP) (for a comprehensive website address for all Human Development Reports that is publicly accessible for free downloads, see http://hdr.undp.org/en/reports/global/hdr2011/). Explicitly, Guillermo O'Donnell (2004a, pp. 11–12) points out: "The concept of human development that has been proposed and widely diffused by UNDP's *Reports* and the work of Amartya Sen was a reversal of prevailing views about development. . . . The concept asks how every individual is doing in relation to the achievement of 'the most elementary capabilities, such as living a long and healthy life, being knowledgeable, and enjoying a decent standard of living'" (O'Donnell 2004a, pp. 11–12; UNDP 2000, p. 20). *If the implementation of O'Donnell is reflected upon the initial questions asked in this contribution for the conceptualization of democracy and the quality of democracy, it can be interpreted but also convincingly argued that "sustainable development" can be suggested as an additional dimension ("basic dimension") for democracy, which would be important for the quality of democracy in a global perspective* (see again Campbell 2012, pp. 296, 301–302, and compare with Campbell 2017). For a systematic attempt of empirical assessment on possible linkages between democracy and development, see Przeworski et al. (2003). As a result of the distinction between dimensions (basic dimensions) for democracy and the quality of democracy, the following proposition is put up for debate: in addition to the dimensions of *freedom*, *equality*, *and control* as being suggested by Lauth (2004, pp. 32–101), *the dimension of sustainable development should be introduced as a fourth dimension* (see again Fig. 1). Regarding suggestions for defining sustainable development, Verena Winiwarter and Martin Knoll (2007, pp. 306–307) commented: "In the meantime, as described, multiple definitions for sustainability exist. A fundamental distinction within the definition lies in the question whether only the relation of society with nature or if additionally social and economic factors should be considered."

There are different theories, conceptual approaches, and models for knowledge production and innovation systems. In the Triple Helix model of innovation, Etzkowitz and Leydesdorff (2000, p. 112) developed a conceptual architecture for innovation, where they tie together the three helices of academia (higher education), industry (business), and state (government). This conceptual approach was extended by Carayannis and Campbell (2009, 2012, p. 14) in the so-called Quadruple Helix model of innovation systems by adding as a fourth helix the "media-based and culture-based public," "civil society," and "arts, artistic research, and arts-based innovation" (Carayannis and Campbell 2014, pp. 6, 15; 2015, pp. 41–42; Bast et al. 2015). *The Quadruple Helix, therefore, is broader than the Triple Helix and contextualizes the Triple Helix,* by interpreting Triple Helix as a core model that is being embedded in and by the more comprehensive Quadruple Helix. *Furthermore, the next-stage model of the Quintuple Helix model of innovation contextualizes the Quadruple Helix, by bringing in a further new perspective by adding additionally the "natural environment" (natural environments) of society.* The Quintuple Helix represents a "five-helix model," "where the environment or the natural environments represent the fifth helix" (Carayannis and Campbell 2010, p. 61). In trying to emphasize, compare, and contrast the focuses of those different Helix innovation

models, we can assert that the Triple Helix concentrates on the knowledge economy, the Quadruple Helix on knowledge society and knowledge democracy, while the Quintuple Helix refers to socioecological transitions and the natural environments (Carayannis et al. 2012, p. 4; see also Carayannis and Campbell 2011). *For explaining and comparing democracy and the quality of democracy, we propose a "Quadruple-dimensional structure" of four different "basic dimensions" of democracy that are being called freedom, equality, control, and sustainable development* (Fig. 1 offers a visualization on these). Here, we actually may draw a line of comparison between concepts and models in the theorizing on democracy and democracy quality and the theorizing on knowledge production and innovation systems. This also opens up a window of opportunity for an interdisciplinary and transdisciplinary approaching of democracy as well as of knowledge production and innovation. *In conceptual terms, the Quadruple-dimensional structure of democracy could also be rearranged (re-architectured) in reference to helices, by this creating a "Model of Quadruple Helix Structures" for democracy and the quality of democracy.* The metaphor and visualization in reference to terms of *helices* emphasize the fluid and dynamic interaction, overlap, and coevolution of the individual dimensions of democracy. As basic dimensions for democracy, we propose (proposed) to identify freedom, equality, control, and sustainable development. Figure 5 introduces a possible visualization from a helix perspective for a theoretical framing of democracy. With respect to further characteristics and trend developments in and of *knowledge democracy*, see also the conceptual framings and discussions in In't Veld and Roeland (2010).

As already being mentioned, equality is often associated closer with left-wing political positions and freedom with right-wing positions. *A measure of performance of political and nonpolitical dimensions in relation to sustainable development has the advantage (especially in the case where sustainable development is understood comprehensively) that this procedure is mostly (often) left/right neutral. Such a measure of performance as a basis of the assessment of democracy and quality of democracy offers an additional reference point ("meta-reference point") outside of usual ideologically based conflict positions* (Campbell 2008, pp. 30–32). It can be argued in a similar manner that the dimension of control mentioned by Lauth (2004, pp. 77–96) positions itself as left-right neutral as well. The definition developed by the "Democracy Ranking" for the quality of democracy is "Quality of Democracy = (freedom & other characteristics of the political system) & (performance on the nonpolitical dimensions)." *The definition is interpreted as a further empirical operationalization step and as a practical application for the measurement of democracy and the quality of democracy respectively which is based on the theory about the quality of democracy by Guillermo O'Donnell*. However, the conceptual democracy formula of the Democracy Ranking has been developed independently (Campbell and Sükösd 2002).

There exist several global initiatives that commit themselves to a regular empirical democracy measurement. It cannot be convincingly argued that there are no data or indicators for a systematically comparative measurement of democracy (at least in the recent years). Of course there can and should be discussions about the quality of these

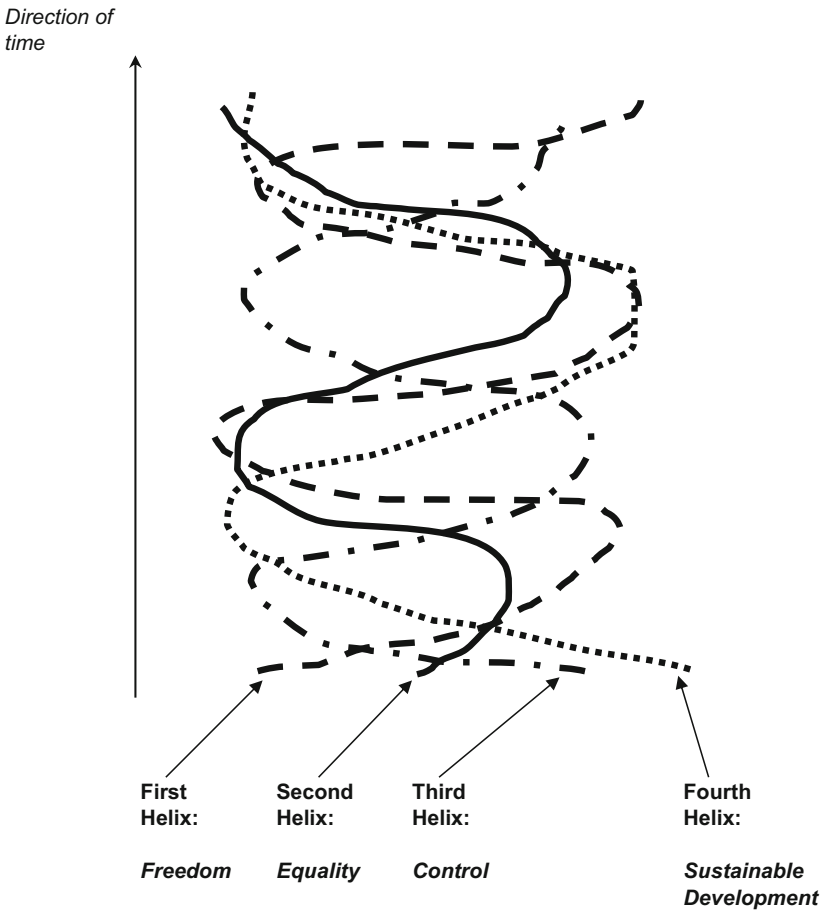


Fig. 5 The Quadruple Helix structure of the basic dimensions of democracy and the quality of democracy (Source: Authors' own conceptualization based on Etzkowitz and Leydesdorff (2000, p. 112), Carayannis and Campbell (2012, p. 14), Danilda et al. (2009), Campbell (2008, p. 32), and for the dimension of "control" on Lauth (2004, pp. 32–101))

data and their cross-references to theory of democracy. The works of Freedom House (see, e.g., Gastil 1993) and of the Democracy Ranking shall be elaborated in more detail during the analysis of the quality of democracy in the United States and in Austria. Other initiatives (without claiming entirety) include Vanhanen's Index of Democracy (Vanhanen 2000) (see http://www.prio.no/CSCW/Datasets/Governance/Vanhanens-index-of-democracy), Polity IV (see http://www.system icpeace.org/polity/polity4.htm), Democracy Index (EIU 2010) (see http://www.eiu.com/public/topical_report.aspx?campaignid=demo2010), and the Democracy Barometer (Bühlmann et al. 2011) (see http://www.democracybarometer.org/). For a comparison of different initiatives, see Pickel and Pickel (2006, pp. 151–277) and Campbell and Barth (2009,

pp. 214–218). The Democracy Barometer provides a "concept tree" ("*Konzeptbaum*") for the quality of democracy which also consists of the three dimensions of freedom, control, and equality: "The Democracy Barometer assumes that democracy is guaranteed by the three principles of Freedom, Control and Equality." The original quote in German is "Das Democracy Barometer geht davon aus, dass Demokratie durch die drei Prinzipien Freiheit, Kontrolle und Gleichheit sichergestellt wird" (see http://www.democracybarometer.org/concept_de.html). A strong resemblance with the three (basic) dimensions of democracy by Lauth (2004, pp. 32–101) is evident in which the talk is also about equality, freedom, and control (Fig. 1).

The *International Institute for Democracy and Electoral Assistance* (International IDEA), established in Stockholm, Sweden, dedicated itself to the approach of the *Democratic Audit* by assessing the quality of democracy (see http://www.idea.int/). IDEA uses its own *State of Democracy (SoD) Assessment Framework* for this purpose which is built on the following two principles: "popular control over public decision-making and decision-makers" and "equality of respect and voice between citizens in the exercise of that control" (IDEA 2008, p. 23). This framework is understood as a further level of operationalization for the democracy assessment of such concepts developed by David Beetham. Beetham (1994, p. 30, 2004) argues that a "complete democratic audit" has to cover the following areas: "free and fair elections," "civil and political rights," "a democratic society," and "open and accountable government." Beetham has been successively involved in various democratic audit processes in the United Kingdom (see, e.g., Beetham et al. 2002), and moreover (at least for the further conceptual development) he is also committed with IDEA (see again IDEA 2008). The assessment framework of IDEA for democracy evaluation has been applied to 21 countries since 2000, however excluding Austria, Germany, and Switzerland (for an overview see http://www.idea.int/sod/worldwide/reports.cfm).

Besides those more globally reaching initiatives of a comparative assessment of quality of democracy, other studies prefer focusing on the democracy of a particular country. For example, Austria represents the type of an advanced small-sized country democracy in Europe, also being a member country to the European Union. To summarize the current status of research and studies regarding the quality of democracy in Austria, the mid-1990s provide a useful starting point. The "*Die Qualität der österreichischen Demokratie*" (*Quality of Democracy in Austria*, by Campbell et al. 1996) represented the first attempt to analyze the Austrian quality of democracy, at least from an academic (and sciences-based) point of view. The next, once again systematic approach of evaluation of the Austrian quality of democracy took place in the "*Demokratiequalität in Österreich*" (*Quality of Democracy in Austria*, by Campbell and Schaller 2002). In the meantime, this book already can be downloaded for free as a whole and complete PDF from the web (visit the following link: http://www.ssoar.info/ssoar/View/?resid=12473). In an exclusive chapter contribution from this volume, an attempt was made to understand or to position the quality of democracy of Austria interactively between basic rights or human rights ("*Grundrechten*") on one hand and power-balancing structures ("*Macht-ausbalancierenden Strukturen*") on the other (Campbell 2002, p. 19).

"*Grundrechte*" here may be interpreted as *human rights* as they are being proposed by Guillermo O'Donnell (2004a, pp. 12, 47). In reference to the already mentioned basic dimensions of democracy and the quality of democracy, the power-balancing structures ("*Macht-ausbalancierenden Strukturen*" or "*Macht-ausgleichenden Strukturen*") may be aligned to the dimension of control (see Lauth 2004, pp. 77–96). Later studies have already started preferring a comparative approach (see Beck and Schaller 2003; Fröschl et al. 2008; Barth 2010, 2011; Campbell 2012, 2015a, b).

The Quality of Democracy in Comparative Perspective: A Comparative Empirical View of the OECD Countries (and EU27 Member Countries) Relating to the Dimensions of Freedom, Equality, Control, and Sustainable Development

The International Comparison (Part One): Focus on the Year 2010

The following session validates the quality of democracy in the OECD (EU27) countries through empirical indicators by providing a comparative approach and analysis in order to create a platform to discuss the propositions for assessing and analyzing quality of democracy (as is being finally attempted in section "Conclusion: Quality of Democracy in Quadruple Helix Structures"). Assessment, even more importantly *evaluation*, is being used here less to provide factual statements but rather more as a stimulant for discussion and to search for possibilities to improve democracy. Evaluation is therefore meant to provoke *democracy learning* ("*Demokratielernen*"). The benchmark for comparison covers all the member states of the OECD, complemented by the remaining member states of the EU27. The chosen time frame is always the last year with available data information (as of early 2012), usually extracted from the year 2010. Partially, in the following Tables 1 and 2, we had to estimate, to which calendar year a specific index year referred to. Only available indicators were used and no new indicators were created. *This emphasized and emphasizes to refer to already existing knowledge*. Indicators being used are from such institutions (organizations) that have a relatively "impartial" ("nonpartisan") reputation but also reflect a certain consensual "mainstream" point of view. Possible critical findings weigh even more for this particular reason. That should also underline that the OECD countries have been well documented regarding indicators over a longer period of time (which does not deny the need for new and even better indicators). *In order to support a comparative analysis and view, all the indicators have been rescaled on a rating spectrum from 0 to 100, in which "0" indicates the worst possible (theoretically and/or empirically) and "100" the best empirical value of measurement for the interpretation of democracy and quality of democracy (in the specific context of our 40-country sample here).* For the process of rescaling the freedom of press and the Gini coefficient, we therefore had to shift reversely the value direction of the primary data, to make values (data) compatible with the other indicators. Results of that rescaling are being represented in Table 1. Data in Table 2

Table 1 Quality of democracy of the United States (USA) in comparison (Part A)

	Political rights (2010)	Civil liberties (2010)	Freedom of press (2010)	Economic freedom (2010)	Gender equality (2010)	Income equality (2009)	Corruption Perceptions Index (2010)	Human Development Index (2010)	Democracy Ranking (2009–2010)	Migrant Integration Policy Index (2010)	MIPEX: access to nationality (2010)
Australia	97.50	95.00	87.78	100.00	85.30	86.91	93.54	98.50	90.02	81.93	93.90
Austria	97.50	96.67	87.78	87.15	83.81	96.73	84.93	93.78	90.48	50.60	26.82
Belgium	97.50	96.67	97.78	85.09	88.15	96.99	76.32	93.89	90.25	80.72	84.14
Bulgaria	87.50	78.33	72.22	78.66	81.70		38.64	81.56	72.25	49.39	29.26
Canada	100.00	98.33	90.00	97.94	86.68	88.48	95.69	96.25	90.37	86.75	90.24
Chile	97.50	96.67	78.89	93.82	82.21	66.23	77.40	85.21	81.31		
Cyprus	95.00	93.33	86.67	88.85	76.71		67.71	88.96	80.62	42.16	39.02
Czech Republic	95.00	95.00	90.00	85.33	79.35	97.38	49.41	91.64	80.39	55.42	40.24
Denmark	100.00	95.00	96.67	95.27	91.08	98.43	100.00	94.86	94.61	63.85	40.24
Estonia	97.50	93.33	91.11	91.15	81.65	89.66	69.86	88.42	81.54	55.42	19.50
Finland	100.00	100.00	100.00	89.70	98.26	96.99	98.92	93.46	97.25	83.13	69.51
France	95.00	95.00	85.56	78.30	82.06	92.54	73.09	93.68	86.24	61.44	71.95
Germany	97.50	95.00	92.22	87.03	88.85	92.28	84.93	95.93	91.63	68.67	71.95
Greece	90.00	83.33	77.78	73.09	80.85	90.71	37.57	91.21	78.90	59.03	69.51
Hungary	92.50	88.33	77.78	80.72	77.60	95.29	50.48	86.39	77.29	54.21	37.80
Iceland	100.00	98.33	97.78	82.66	100.00	91.49	91.39	95.18			
Ireland	97.50	96.67	93.33	95.39	91.70	92.54	86.01	96.25	91.74	59.03	70.73
Israel	90.00	78.33	78.89	83.03	80.97	82.33	65.55	94.11	82.45		
Italy	92.50	86.66	73.33	73.09	79.43	86.78	41.87	92.60	80.28	72.29	76.83
Japan	92.50	85.00	87.78	88.24	76.09	87.83	83.85	95.50	83.83	45.78	40.24
Korea	90.00	83.33	75.56	84.60	73.32	89.66	58.02	95.07	79.36		
Latvia	82.50	86.66	82.22	79.76	86.58		46.18	85.21	77.64	37.34	18.28

(*continued*)

Table 1 (continued)

	Political rights (2010)	Civil liberties (2010)	Freedom of press (2010)	Economic freedom (2010)	Gender equality (2010)	Income equality (2009)	Corruption Perceptions Index (2010)	Human Development Index (2010)	Democracy Ranking (2009–2010)	Migrant Integration Policy Index (2010)	MIPEX: access to nationality (2010)
Lithuania	92.50	88.33	86.67	86.42	83.40		53.71	85.74	79.70	48.19	24.38
Luxembourg	100.00	100.00	97.78	92.36	84.41	93.19	91.39	91.85		71.08	80.49
Malta	97.50	96.67	86.67	79.63	77.79		60.17	88.10		44.57	31.70
Mexico	72.49	61.66	42.22	82.18	77.15	68.59	33.26	81.46	63.88		
Netherlands	100.00	96.67	95.56	90.54	87.43	92.41	94.62	96.46	93.58	81.93	80.49
New Zealand	97.50	96.67	94.44	99.76	91.46	87.70	100.00	96.25	93.92		
Norway	100.00	100.00	98.89	85.21	98.51	98.17	92.47	100.00	100.00	79.52	49.99
Poland	95.00	91.67	83.33	77.69	82.30	90.97	56.94	86.07	79.70	50.60	42.68
Portugal	97.50	96.67	92.22	77.57	83.56	84.69	64.48	85.64	85.67	95.18	100.00
Romania	85.00	81.66	64.44	78.42	79.62		39.72	82.64	71.56	54.21	35.36
Slovak Republic	92.50	88.33	86.67	84.24	79.44	97.25	46.18	88.32	76.95	43.37	32.92
Slovenia	95.00	88.33	83.33	78.30	82.34	100.00	68.78	93.68	85.09	59.03	40.24
Spain	100.00	95.00	85.56	85.09	88.73	89.40	65.55	93.03	87.84	75.90	47.55
Sweden	100.00	100.00	98.89	87.15	94.23	96.99	98.92	95.82	98.85	100.00	96.34
Switzerland	97.50	95.00	96.67	99.27	89.29	91.23	93.54	95.71	96.56	51.80	43.90
Turkey	67.49	59.99	51.11	77.82	69.44	77.36	47.26	73.85	58.94		
UK	100.00	95.00	90.00	90.30	87.33	85.73	81.70	91.43	90.48	68.67	71.95
USA	95.00	93.33	92.22	94.30	86.74	81.41	76.32	96.46	89.45	74.70	74.39
Mean (unweighted)	**94.25**	**91.00**	**85.69**	**86.13**	**84.39**	**89.83**	**70.91**	**91.25**	**84.61**	**63.81**	**55.83**

Source: Authors' own rescaling based on original sources (see text for source citation)
Scale range 0–100, 0 = lowest possible (theoretical and/or empirical) value, 100 = highest empirical value

Table 2 Quality of democracy of the United States (USA) in comparison (Part B)

	Political rights (2010)	Civil liberties (2010)	Freedom of press (2010)	Economic freedom (2010)	Gender equality (2010)	Income equality (2009)	Corruption Perceptions Index (2010)	Human Development Index (2010)	Democracy Ranking (2009–2010)	Migrant Integration Policy Index (2010)	MIPEX: access to nationality (2010)
Australia	92.31	87.50	78.85	100.00	51.90	61.24	90.32	94.26	75.70	71.15	92.54
Austria	92.31	91.67	78.85	52.25	47.01	90.31	77.42	76.23	76.82	21.15	10.45
Belgium	92.31	91.67	96.15	44.59	61.22	91.09	64.52	76.64	76.26	69.23	80.60
Bulgaria	61.54	45.83	51.92	20.72	40.10		8.06	29.51	32.40	19.23	13.43
Canada	100.00	95.83	82.69	92.34	56.41	65.89	93.55	85.66	76.54	78.85	88.06
Chile	92.31	91.67	63.46	77.03	41.77	0.00	66.13	43.44	54.47		
Cyprus	84.62	83.33	76.92	58.56	23.80		51.61	57.79	52.79	7.69	25.37
Czech Republic	84.62	87.50	82.69	45.50	32.41	92.25	24.19	68.03	52.23	28.85	26.87
Denmark	100.00	87.50	94.23	82.43	70.81	95.35	100.00	80.33	86.87	42.31	26.87
Estonia	92.31	83.33	84.62	67.12	39.95	69.38	54.84	55.74	55.03	28.85	1.49
Finland	100.00	100.00	100.00	61.71	94.29	91.09	98.39	75.00	93.30	73.08	62.69
France	84.62	87.50	75.00	19.37	41.30	77.91	59.68	75.82	66.48	38.46	65.67
Germany	92.31	87.50	86.54	51.80	63.51	77.13	77.42	84.43	79.61	50.00	65.67
Greece	69.23	58.33	61.54	0.00	37.34	72.48	6.45	66.39	48.60	34.62	62.69
Hungary	76.92	70.83	61.54	28.38	26.71	86.05	25.81	47.95	44.69	26.92	23.88
Iceland	100.00	95.83	96.15	35.59	100.00	74.81	87.10	81.56			
Ireland	92.31	91.67	88.46	82.88	72.83	77.91	79.03	85.66	79.89	34.62	64.18
Israel	69.23	45.83	63.46	36.94	37.73	47.67	48.39	77.46	57.26		
Italy	76.92	66.67	53.85	0.00	32.69	60.85	12.90	71.72	51.96	55.77	71.64
Japan	76.92	62.50	78.85	56.31	21.74	63.95	75.81	82.79	60.61	13.46	26.87
Korea	69.23	58.33	57.69	42.79	12.69	69.38	37.10	81.15	49.72		
Latvia	46.15	66.67	69.23	24.77	56.09		19.35	43.44	45.53	0.00	0.00

(*continued*)

Table 2 (continued)

	Political rights (2010)	Civil liberties (2010)	Freedom of press (2010)	Economic freedom (2010)	Gender equality (2010)	Income equality (2009)	Corruption Perceptions Index (2010)	Human Development Index (2010)	Democracy Ranking (2009–2010)	Migrant Integration Policy Index (2010)	MIPEX: access to nationality (2010)
Lithuania	76.92	70.83	76.92	49.55	45.69		30.65	45.49	50.56	17.31	7.46
Luxembourg	100.00	100.00	96.15	71.62	48.99	79.84	87.10	68.85		53.85	76.12
Malta	92.31	91.67	76.92	24.32	27.33		40.32	54.51		11.54	16.42
Mexico	15.38	4.17	0.00	33.78	25.23	6.98	0.00	29.10	12.01		
Netherlands	100.00	91.67	92.31	64.86	58.85	77.52	91.94	86.48	84.36	71.15	76.12
New Zealand	92.31	91.67	90.38	99.10	72.05	63.57	100.00	85.66	85.20		
Norway	100.00	100.00	98.08	45.05	95.11	94.57	88.71	100.00	100.00	67.31	38.81
Poland	84.62	79.17	71.15	17.12	42.08	73.26	35.48	46.72	50.56	21.15	29.85
Portugal	92.31	91.67	86.54	16.67	46.20	54.65	46.77	45.08	65.08	92.31	100.00
Romania	53.85	54.17	38.46	19.82	33.31		9.68	33.61	30.73	26.92	20.90
Slovak Republic	76.92	70.83	76.92	41.44	32.73	91.86	19.35	55.33	43.85	9.62	17.91
Slovenia	84.62	70.83	71.15	19.37	42.20	100.00	53.23	75.82	63.69	34.62	26.87
Spain	100.00	87.50	75.00	44.59	63.12	68.60	48.39	73.36	70.39	61.54	35.82
Sweden	100.00	100.00	98.08	52.25	81.13	91.09	98.39	84.02	97.21	100.00	95.52
Switzerland	92.31	87.50	94.23	97.30	64.95	74.03	90.32	83.61	91.62	23.08	31.34
Turkey	0.00	0.00	15.38	17.57	0.00	32.95	20.97	0.00	0.00		
UK	100.00	87.50	82.69	63.96	58.54	57.75	72.58	67.21	76.82	50.00	65.67
USA	84.62	83.33	86.54	78.83	56.60	44.96	64.52	86.48	74.30	59.62	68.66
Mean (unweighted)	**82.31**	**77.50**	**75.24**	**48.46**	**48.91**	**69.89**	**56.41**	**66.56**	**62.52**	**42.25**	**45.95**

Source: Authors' own rescaling based on original sources (see text for source citation)
Scale range 0–100, 0 = lowest empirical value, 100 = highest empirical value

are arranged somewhat differently: there, the highest observed empirical value still is 100; "0," however, is not the lowest possible value, but the lowest empirically observed value. Therefore, put in contrast, a comparison of the indicators in Tables 1 and 2 should allow for a better and more nuanced interpretation of the different countries and their quality of democracy (OECD, EU27). Mean values in Tables 1 and 2 are not weighted by population. Acronyms in Tables 1 and 2 have the following meaning: USA = United States and UK = United Kingdom. The comparison is based on a total of 11 indicators, in which the majority (more or less) fits nicely or at least convincingly into the 4 identified (basic) dimensions of democracy (see Fig. 1 in section "Conceptualizing Democracy and the Quality of Democracy: Freedom, Equality, Control, and Sustainable Development (Model of Quadruple Helix Structures)"). Such a broad indicator spectrum is used for an attempt "to determine a multi-layered quality profile of democracies" and could thus help, as put up for discussion by Hans-Joachim Lauth (2011, p. 49), to develop "qualitative or complex approaches for democracy measurement." In the subsequent Tables 1 and 2, the empirical results are provided, and in what follows, the exact sources of indicators are being displayed and presented:

1. *The dimension of freedom*: For this, *political rights*, *civil liberties*, and *freedom of press* are used as indicators as drawn up yearly by the Freedom House (2011c, d). Civil liberties play an important role, as they help allocate systems between primary *electoral democracies* and *liberal democracies* (with a higher quality of democracy). For political rights and civil liberties, the differentiated "aggregate and subcategory scores" are accessed. In some cases, controversial discussions take place concerning the reliability of Freedom House. But it appears that the methodology being used by Freedom House in the previous years has improved and Freedom House operates through a peer-review process that corresponds to the basic academic standards (Freedom House 2011a). Also, the Freedom House data related to OECD countries are less problematic than the data available regarding non-OECD countries. Moreover, Freedom House rates freedom in multiple countries as higher than that prevailing in the United States itself (see also the discussion by Pickel and Pickel 2006, p. 221). Additionally, data from the *Index of Economic Freedom* have been added (Heritage Foundation 2011). Regarding economic freedom, there appears to be a conflict or dilemma whether this should influence an evaluation measure (of freedom) of the quality of democracy.
2. *The dimension of equality*: The choice rests on two indicators in this case. Regarding gender equality, the *Global Gender Gap Index* is referred to, as is being published annually by the World Economic Forum (Hausmann et al. 2011). As a comprehensive measure for gender equality, it covers the following areas: "economic participation and opportunity," "educational attainment," "health and survival," and "political empowerment." With respect to income equality, the *Social and Welfare Statistics* of the OECD (2011) are used for reference. Concerning the distribution of income, we decided to employ the "Gini coefficient" for the total population ("after taxes and transfers," as the respective OECD

source indicates; OECD 2011). The Gini coefficient is also known as the "Gini index." Concerning the Gini coefficient (rescaled as income equality) in Tables 1 and 2, we interpreted 2009 as the approximate year of reference for the calendar year. The OECD online database (OECD 2011) speaks in this respect of the "late 2000s."

3. *The dimension of control*: The *Corruption Perceptions Index* (CPI) is used in this regard, which is published yearly by Transparency International (2011). The CPI aggregates different opinion surveys and ranks countries according to the perceived level of corruption in a country. Corruption is (indirectly) used as an interpretation tool to measure the extent as to which the dimension of control is functioning (or not). The higher the values (data) for the Corruption Perceptions Index in Tables 1 and 2, the lower are the levels of perceived corruption.
4. *The dimension of sustainable development*: The first choice rests on the *Human Development Index* (HDI), which is published regularly by the United Nations Organization (UNDP 2011). The HDI is calculated using the following dimensions: "long and healthy life," "knowledge," and "a decent standard of living." The HDI therefore measures *human development*, which is one of the two basic principles that combine together with *human rights* to provide and explain the theoretical foundation and theoretical architecture of Guillermo O'Donnell (2004a) regarding the quality of democracy. As a second indicator, the aggregated "total scores" of the Democracy Ranking (2011) are considered. The *Democracy Ranking* 2011 calculates the average means for the years 2009–2010 and aggregates the different dimensions in the following way (Campbell 2008, p. 34): *politics* 50% and 10% each for *gender*, *economy*, *knowledge*, *health*, and *environment* (see also: http://www.democracyranking.org/en/). Thereby, the Democracy Ranking defines and analyzes sustainable development even more comprehensively than the HDI (Human Development Index). The ". . .*Democracy Ranking displays what happens when the freedom ratings of Freedom House and the Human Development Index of the United Nations Development Program are being pooled together into a comprehensive picture*"(Campbell 2011, p. 3).
5. *Other indicators*: Two indicators of the *Migrant Integration Policy Index* (MIPEX) are adopted in comparing the quality of democracy (Huddleston et al. 2011): The "overall score (with education)" as well as the "access to nationality." This index therefore measures the integration of immigrants and noncitizens, respectively, in a society and democracy. At first glance, it is not completely clear in which aforementioned dimensions (freedom, equality, control, and sustainable development) should the MIPEX be allocated. The possibility of multiple allocations is conceivable.

The International Comparison (Part Two): Comparison of the Years 2011–2012 and 2014–2015

The Democracy Ranking (http://democracyranking.org/wordpress/) represents an approach that tries to measure and compare quality of democracy in a global format

and by applying a scientific model. For that purpose, quality of democracy refers to different dimensions (with different weights), and to those different dimensions, different indicators are being assigned. All indicator scores are transformed into a value (score) range of 1–100, where 1 implies the lowest and 100 the highest value (for quality of democracy). Normally, the Democracy Ranking compares two intervals of double years (where average values are being drawn for every double-year segment) (Campbell 2008).

More specifically, the Democracy Ranking 2016 compares the development of quality of democracy in 112 countries for the (two double) years 2011–2012 and 2014–2015. It is based on the following dimensions: politics (weighted with 50%), economy (10%), ecology and environment (10%), gender equality (10%), health and health status (10%), and knowledge (10%). The possible values that a country can achieve extend from 1 (the observed empirical minimum) to 100 (the observed empirical maximum) (the entire scale is thus 1–100).

The following key results of the Democracy Ranking 2016 should be emphasized (Campbell et al. 2017):

1. *The ten top-ranked countries for 2014–2015 are* Norway (100.00), Switzerland (99.49), Sweden (98.45), Finland (98.04), Denmark (96.61), the Netherlands (93.41), New Zeeland (90.26), Germany (90.30), Ireland (89.57), and Australia (88.74).
2. *Improvement Ranking, the increase of quality of democracy*: A relatively large progress (although often resulting from a lower level) was in several African countries (Ivory Coast, Madagascar, Senegal, and Burkina Faso), in Latin American in Nicaragua and Columbia, as well as in Tunisia. Tunisia is the only country of the Arab Spring that could realize a positive (and by tendency stable) path to more democracy.
3. *Improvement Ranking, the decrease of quality of democracy*: A decrease can be observed for all the other countries of the Arab Spring (e.g., Libya and Egypt), as well as for Venezuela (in contrast to Columbia), and within the EU for Hungary. Furthermore the decrease of democracy in Turkey is remarkable and obvious. In Russia and China, the quality of the political systems has also decreased.
4. *Austria*: Austria increased its scoring from 86.54 (2011–2012) to 87.76 (2014–2015) but slipped down slightly from rank 12 (2011–2012) to rank 13 (2014–2015). In international comparison, Austria ranks very high (rank 13 from 112 countries). However, a few of the other top-rated countries developed during the last years a faster dynamics than Austria. Freedom House rated the political rights for Austria during 2014–2015 stricter than still for 2011–2012.
5. *Possibly approaching problem region of the Balkans*: The results of the Democracy Ranking also can be used in the sense of an early warning system for possibly arising problem situations. Serbia achieved an increase in quality of democracy (in the areas of politics, economy, and society), yet apparently not enough to improve its negotiation position for an EU membership. In Bosnia-Herzegovina and Macedonia, the scoring for economy and society improved, but in the area of politics, there was a decrease. Albania could increase

its scoring for politics and society, but there was a decrease in economy. These recent trends in Bosnia-Herzegovina, Macedonia, and Albania require a more intensive international attention and observation.

Selected results of the Democracy Ranking 2016 (for the OECD and EU member countries) are summarized in Tables 3 and 4. Value scores have been adjusted to a value spectrum from "0" to "100," where 0 represents the lowest observed empirical value and 100 the highest observed empirical value (for the completely covered time period of 2011–2012 and 2014–2015). Also changes in the quality of democracy scorings are indicated (improvements but also decreases).

Conclusion: Quality of Democracy in Quadruple Helix Structures

Conclusion (Part One): Comparative Assessment and First Evaluation of Quality of Democracy in OECD Countries and the EU27 Member Countries

The following three research questions governed the analytical procedure of this chapter:

1. To develop (in fact to prototype) a conceptual framework of analysis for a global comparison of quality of democracy. This framework will also reference to the concept of the Quadruple Helix innovation systems.
2. In a second step, to use and to test this same conceptual framework for a comparative measurement of quality of democracy in the different OECD and EU27 member countries.
3. In a final step, and based on the previous conceptual and comparative analysis, quality of democracy propositions for a democracy reform are being developed for democracy in Austria.

In theoretical and conceptual terms, we referred to a Quadruple-dimensional structure, also a Quadruple Helix structure (a "Model of Quadruple Helix Structures") of the four basic dimensions of freedom, equality, control, and sustainable development, for explaining and comparing democracy and the quality of democracy.

What comes to mind, when looking at quality of democracy in reference to OECD and EU member countries, is the comparatively high ranking and positioning of the Nordic countries in Europe, particularly Norway, Sweden, Finland, and Denmark (see also on the web the newest and most recent scores of the Democracy Ranking 2016: http://democracyranking.org/wordpress/2016-full-dataset/). Also Switzerland places very high. The Nordic countries and Switzerland are also a good example for sustainable development, because they achieved and realized a development across different dimensions and indicators, so their progress is well-balanced. Of course, from a philosophical perspective, we always could speculate

Table 3 Quality of democracy in OECD and EU member countries in the years 2011–2012 and 2014–2015 in comparison. Countries ranked alphabetically (Part A)

	Years 2011–2012	Years 2014–2015	Changes in scores
Australia	88.02	88.74	0.72
Austria	86.54	87.76	1.22
Belgium	86.23	88.44	2.22
Bulgaria	58.64	61.82	3.18
Canada	86.92	87.62	0.71
Chile	72.70	74.26	1.56
Cyprus	69.77	69.22	−0.55
Czech Republic	71.81	74.11	2.30
Denmark	94.96	96.61	1.65
Estonia	70.89	74.91	4.02
Finland	97.60	98.04	0.44
France	81.80	85.10	3.30
Germany	88.92	90.30	1.38
Greece	64.70	63.40	−1.30
Hungary	63.12	61.11	−2.01
Iceland			
Ireland	86.80	89.57	2.77
Israel	73.41	74.85	1.45
Italy	70.59	73.06	2.47
Japan	75.97	80.34	4.37
Korea	70.84	71.73	0.89
Latvia	67.64	72.20	4.56
Lithuania	71.70	75.17	3.47
Luxembourg			
Malta			
Mexico	45.48	47.78	2.30
Netherlands	92.26	93.41	1.15
New Zealand	89.89	90.26	0.38
Norway	99.55	100.00	0.45
Poland	70.94	73.14	2.20
Portugal	77.52	78.75	1.23
Romania	60.22	62.69	2.47
Slovak Republic	67.09	67.42	0.33
Slovenia	77.25	81.18	3.93
Spain	81.33	79.85	−1.48
Sweden	96.89	98.45	1.56
Switzerland	97.81	99.49	1.68
Turkey	44.20	39.55	−4.65
UK (United Kingdom)	84.78	87.33	2.55

(*continued*)

Table 3 (continued)

	Years 2011–2012	Years 2014–2015	Changes in scores
USA (United States)	82.13	82.22	0.09
Mean (unweighted and without Syria)	**77.48**	**78.92**	**1.43**
Syria	4.27	0.00	−4.27

Methodic note: scoring extends from 0 (the lowest observed democracy value) to 100 (the highest observed democracy value). In the country sample, Norway (2014–2015) ranks highest, and Syria (2014–2015) ranks lowest

Source: Authors' own calculations based on the Democracy Ranking 2016 (Campbell et al. 2017)

"how high is the high" of quality of democracy in the Nordic countries and in Switzerland from a "really timeless viewpoint." But in "relative" empirical terms, no country or no democracy places higher than the Nordic countries and Switzerland (so far). So they define a practical and pragmatic benchmark for quality of democracy that already is accomplishable by countries. "The Nordic democracies (and Switzerland) demonstrate in empirical terms and in practice, which degrees and levels of a quality of democracy already can be achieved at the beginning of the twenty-first century" (Campbell 2011, p. 6).

In the following, we provide a first assessment for the quality of democracy in the United States, based on the empirical data that is strictly and consistently comparative in nature and character, and put forward first propositions. For the comparative assessment of the quality of democracy in the United States we can formulate the following tentative propositions. The United States ranks highest on the Human Development Index (dimension of sustainable development) and on political rights, economic freedom, civil liberties, and freedom of press, which means all dimension of freedom. Concerning the dimension of equality, the scoring of the United States is not that good anymore. With regard to gender equality, the United States positions itself slightly above OECD average, but concerning income equality, the United States performs clearly below OECD average. Concerning the perceived corruption, we already asserted that this indicator could be assigned to the dimension of control. In reference to the Corruption Perceptions Index, the United States scores higher (meaning to have less perceived corruption) than the OECD average but behind several of the more developed OECD countries. Concerning the data of the Democracy Ranking 2011 (dimension of sustainable development), the United States performs clearly above the OECD average. On the Migrant Integration Policy Index (MIPEX), the United States also scores above OECD average. *Put in summary, we may conclude: the comparative strengths of the quality of democracy in the United States focus on the dimension of freedom and on the dimension of sustainable development. Further containment of corruption marks potentially a sensitive area and issue for the United States. The comparative weakness of the quality of American democracy lies in the dimension of equality, most importantly income*

Table 4 Quality of democracy in OECD and EU member countries in the years 2011–2012 and 2014–2015 in comparison. Countries ranked based on scores (years 2014–2015) (Part B)

	Years 2011–2012	Years 2014–2015	Change in scores
Norway	99.55	100.00	0.45
Switzerland	97.81	99.49	1.68
Sweden	96.89	98.45	1.56
Finland	97.60	98.04	0.44
Denmark	94.96	96.61	1.65
Netherlands	92.26	93.41	1.15
Germany	88.92	90.30	1.38
New Zealand	89.89	90.26	0.38
Ireland	86.80	89.57	2.77
Australia	88.02	88.74	0.72
Belgium	86.23	88.44	2.22
Austria	86.54	87.76	1.22
Canada	86.92	87.62	0.71
UK (United Kingdom)	84.78	87.33	2.55
France	81.80	85.10	3.30
USA (United States)	82.13	82.22	0.09
Slovenia	77.25	81.18	3.93
Japan	75.97	80.34	4.37
Spain	81.33	79.85	−1.48
Portugal	77.52	78.75	1.23
Lithuania	71.70	75.17	3.47
Estonia	70.89	74.91	4.02
Israel	73.41	74.85	1.45
Chile	72.70	74.26	1.56
Czech Republic	71.81	74.11	2.30
Poland	70.94	73.14	2.20
Italy	70.59	73.06	2.47
Latvia	67.64	72.20	4.56
Korea	70.84	71.73	0.89
Cyprus	69.77	69.22	−0.55
Slovak Republic	67.09	67.42	0.33
Greece	64.70	63.40	−1.30
Romania	60.22	62.69	2.47
Bulgaria	58.64	61.82	3.18
Hungary	63.12	61.11	−2.01
Mexico	45.48	47.78	2.30
Turkey	44.20	39.55	−4.65
Iceland			
Luxembourg			

(*continued*)

Table 4 (continued)

	Years 2011–2012	Years 2014–2015	Change in scores
Malta			
Mean (unweighted and without Syria)	**77.48**	**78.92**	**1.43**
Syria	4.27	0.00	−4.27

Methodic note: scoring extends from 0 (the lowest observed democracy value) to 100 (the highest observed democracy value). In the country sample, Norway (2014–2015) ranks highest, and Syria (2014–2015) ranks lowest

Source: Authors' own calculations based on the Democracy Ranking 2016 (Campbell et al. 2017)

equality. Income inequality defines and represents a major challenge and concern for democracy in the United States.

A different approach is to compare democracy in the United States ("American democracy") not only with other individual (European) countries but with larger political-spatial entities, for example, an indicator-based aggregation of all of the member countries to the European Union (EU27), creating or approximating by this a version of "European democracy." In that sense the whole United States also resembles an "aggregation"; therefore, it makes additionally sense to compare the United States with an aggregation of the EU member countries. Thought about this from a different angle, it also would be possible to compare the different (50) states of the United States individually with the different (national) member countries to the European Union. For the particularly aggregated comparison, we can propose a series of different propositions. It appears that US democracy is leading with regard to freedom and European democracy with regard to equality. While results for political freedom and gender equality are more mixed, the results for economic freedom and income equality are clearly more evident. In terms of economic freedom, the United States is ahead of (aggregated) Europe, and in terms of income equality, (aggregated) Europe is ahead of the United States (Campbell 2013). On political freedom and income equality, the EU15 is internationally more competitive than the EU27 (Campbell 2013, pp. 336, 340).

Does this mean that American democracy has specialized more on realizing freedom, while European democracy (despite national variations) places a greater emphasis on equality? Does this furthermore mark "archetypical" differences in political philosophy? Within the international system of global democracy, different democracies may have placed a different emphasis on different dimensions of quality of democracy, producing perhaps complementary effects for the overall worldwide further development of democracy. What is more important for democracy and quality of democracy, freedom or equality? Again in the long run, obviously, both dimensions, freedom and equality, matter, particularly for contributing to the perspective (dimension) of sustainable development. These differences in American and European democracy also stress the opportunity but also the real need of democracies, to learn mutually from each other (also as an expression of advanced political culture).

The following final propositions (in context of our current analysis here) can be put forward for further discussion for the further development of discourses that are interested to intertwine ("*Inter-Helix*") quality of democracy with innovation and innovation systems:

1. *The basic Quadruple-dimensional structure of democracy and quality of democracy*: The Quadruple Helix structure of quality of democracy identifies four basic (conceptual) dimensions for quality of democracy: freedom, equality, control, and sustainable development (Fig. 1). *Particularly sustainable development marks here a new and innovative contribution to theory of democracy.* Sustainable development also helps to avoid that models of measurement of democracy are biased toward a left-leaning or right-leaning ideological pole of political preferences. Sustainable development adds the important contribution of a more "neutral left/right balance" (Fig. 2). *For sustainable development, knowledge and innovation play an important role, thus fostering the coming together of knowledge society, knowledge economy, and knowledge democracy.* Components of knowledge can be research, education, and innovation (Campbell and Carayannis 2013b; Carayannis and Campbell 2012).
2. *Quadruple Helix of quality of democracy and of innovation systems*: Quadruple Helix qualifies as a concept with interdisciplinary and transdisciplinary capacities and capabilities. Quadruple Helix refers to the basic (conceptual) dimensions of democracy and quality of democracy. Quadruple Helix also represents the architecture of Quadruple and Quintuple Helix innovation systems, demonstrating, how knowledge and innovation processes in mature and advanced innovation systems are being progressed. Quadruple Helix fulfills here at least two crucial functions. (a) *Knowledge and innovation are being defined as key for sustainable development and for the further evolution of quality of democracy.* Knowledge and innovation are receiving an additional meaning and importance for democracy and theory of democracy. How to innovate (and reinvent) knowledge democracy? Democracy discourses and innovation discourses develop further in mutual cross-reference. (b) The other crucial function of the Quadruple Helix is that it demonstrates that the context of society and of democracy is important for innovation systems (Campbell and Carayannis 2016). *The unfolding of an innovative knowledge economy also requires (at least in a longer perspective) the unfolding of a knowledge democracy.* So there is also a "perspective of democracy" for advancing innovation systems. "Democracy of knowledge" plays in both ways (Carayannis and Campbell 2012).
3. *There is no Quadruple or Quintuple Helix innovation system without a democracy*: Pre-Quadruple Helix innovation systems (such as the Triple Helix) can be applied in very different political environments. Triple Helix is possible in combination with democratic or nondemocratic political regimes. The Quadruple Helix is here more specific and concrete. *The architectures of Quadruple Helix and Quintuple Helix innovation systems demand and require the formation of a democracy, implicating that quality of democracy provides for a nurturing of innovation and innovation system, so that quality of democracy and*

progress of innovation mutually "Cross Helix" in a connecting and amplifying mode and manner. In a win-win scenario, quality of democracy, and innovation systems, they both cross-link and coevolve. "The way how the Quadruple Helix is being engineered, designed, and architected clearly shows that there cannot be a Quadruple Helix innovation system without democracy or a democratic context" (Carayannis and Campbell 2014, p. 19). This relates research on quality of democracy to research on innovation (innovation systems) and knowledge economy (see also Carayannis et al. 2018). The one matters for the other. "*Cyber-democracy*" receives here a new meaning (Campbell and Carayannis 2014).

Conclusion (Part Two): Recommended Measures for Improving Quality of Democracy Reform in Austria

There are several analyses that reflect on Austrian democracy and the Austrian political system by referring (in greater detail) to a wider spectrum of themes: Beetham (1994), Campbell (2002, pp. 30–31, 39; 2007, pp. 392–393, 402; 2011; 2015b), IDEA (2008), Müller and Strøm (2000, p. 589), Pelinka (2008), Pelinka and Rosenberger (2003), Poier (2001), Rosenberger (2010), Sickinger (2009), Valchars (2006), and Wineroither (2009).

We want to focus now more specifically on Austrian democracy. *For an assessment (evaluation) of the quality of democracy in Austria, we set up for discussion the following propositions in context of a dynamic thesis formulation* (furthermore, see also Campbell 2015a, b):

1. *Comparatively, Austria's quality of democracy yields good results in* political rights and civil liberties (dimension of freedom), income equality (dimension of equality), and within both indicators for the dimension of sustainable development.
2. *Comparatively, Austria's quality of democracy yields less good results in* freedom of press and economic freedom (dimension of freedom), gender equality (dimension of equality), and corruption (dimension of control).
3. *Comparatively, Austria's quality of democracy yields lower-ranking results in* both indicators used in the Migrant Integration Policy Index (MIPEX) that show a problematic positioning. Austria's comprehensive rank in the MIPEX is only at 26 out of 33 (here are behind Austria only Bulgaria, Lithuania, Japan, Malta, the Slovak Republic, Cyprus, and Latvia), and in the category of access to citizenship, Austria ranks only at 30 out of 33 (here, only Lithuania, Estonia, and Latvia perform poorer than Austria) (see Tables 1 and 2). However, in relation to this observation, it must be noted that the poor performance of Austria in the MIPEX is not negatively reflected by the Freedom House's freedom rating in the category of political rights and civil liberties. One proposition would be that the integration of foreigners and of noncitizens (but being born and living exactly in the country, where they are) is not given enough weight (by Freedom House).

The comparative strengths and weaknesses of the Austrian quality of democracy blend themselves differently along the dimensions of freedom and equality. Regarding sustainable development, Austria's quality of democracy finds itself ranked highly, and its position remains robust. Taking the ratings of the Democracy Ranking during the years 2009 and 2010 under consideration (Democracy Ranking 2011), countries like Norway, Sweden, Finland, and Switzerland find themselves worldwide on top in the category of sustainable development. *Therefore, currently, the Nordic countries provide the global empirical benchmark for democracy development (for a comprehensive and sustainable democracy development). The Nordic countries have impressively demonstrated the level for the quality of democracy that is empirically already possible to achieve*. "The Nordic democracies (and Switzerland) demonstrate in empirical terms and in practice, which degrees and levels of a quality of democracy already can be achieved at the beginning of the twenty-first century" (Campbell 2011, p. 6).

As compared with the OECD countries, the quality of democracy in Austria is ranked high to very high, but not in all dimensions and for all indicators. *Evidently, for the purpose of a further learning with respect to the quality of democracy in Austria (so the proposition), the identification of the potentially problematic areas appears to be relevant above all, since, naturally, those areas require democratic and political reform*. In Austria, necessity for innovation and *democracy innovation* is drastically needed in freedom of press, in gender equality, and in fighting and containing corruption. However, the most urgent action plan for Austria's quality of democracy needs to be implemented particularly in the improvement of integration of immigrants and of non-EU citizens and a better access to citizenship. Integration policy is also linked, interlinked and cross-linked with other policy fields such as asylum policy (Rosenberger 2010). Austria's citizenship law knows no *jus soli* but is directed and steered by a pure *jus sanguinis* policy. Automatic acquisition of Austrian citizenship still only takes place through the Austrian citizenship of the parents (*jus sanguinis*), whereas birth in Austria (*jus soli*), also residence during childhood and youth, are being completely ignored. Persons, who are not Austrian citizens, of course can always apply for Austrian citizenship (when specific conditions are being met and fulfilled), but this is something else than an automatic acquisition of citizenship. *Therefore, descent (in essence also a biological principle) actually decides about political rights and automatic political participation in Austrian democracy. This only can be hardly balanced with the developed quality standards of a democracy in the twenty-first century and, when given further thought, stands finally in contradiction to fairness and universal equality of people and the general application of human rights*. According to Pelinka (2008), there is a need in Austria for a more systematic conceptual reflection on the *demos*, in the sense of "Who are the People?" ("Wer ist das Volk?"). This reflection should definitely encourage more inclusion (see also Valchars 2006). Reforms in citizenship law in other European countries (such as in Germany), in the recent years, did not enter into Austrian politics and were not taken up by the Austrian mainstream political discourses. Should Austrian politics continue the blocking of an introduction of a *jus soli* component into its citizenship law during the course of the coming

years, then it cannot be ruled out completely that the pure *jus sanguinis* design will finally be challenged legally at a "constitutional court" (nationally, supranationally, or even internationally). Here we can quote also from an original source: "Bedenklich für Demokratiequalität ist, wenn ein bedeutender Anteil der Wohnbevölkerung nicht im Besitz der Staatsbürgerschaft ist beziehungsweise sich dieser Anteil sogar vergrößert: Denn das könnte dazu führen, dass manche Parteien, die an Wahlstimmenmaximierung interessiert sind, den StaatsbürgerInnen 'auf Kosten' der Nicht-StaatsbürgerInnen Wahlversprechen geben. … Je größer der Anteil der Nicht-StaatsbürgerInnen, desto höher fällt das populistische Potenzial für den Parteienwettbewerb aus. Soll gegen Populismus ein effektiver Riegel vorgeschoben werden, müsste der Anteil der Nicht-StaatsbürgerInnen an der Wohnbevölkerung möglichst verringert werden" (Campbell, 2002, pp. 30–31).

The following possibilities for a betterment and *quality of democracy reform* of Austrian democracy and politics are to be sketched and presented for a qualified (and necessary) discussion:

1. *Citizenship*: The introduction of an equal and equitable *jus soli* component in Austrian citizenship law, parallel to the current *jus sanguinis* component, appears to be absolutely necessary. *Jus soli* would at least imply that a person, who has been born in Austria, is being regarded automatically as an Austrian citizen. Sufficient residence in years during childhood and youth may also be acknowledged. To address the possibility of dual and multiple citizenship, different scenarios are conceivable and naturally legitimate; there are, however, good arguments in favor of introducing and approving dual and multiple citizenship.
2. *Gender equality, freedom of the press, better integration of immigrants (non-EU citizens), and containment of corruption*: These are areas and policy fields of concern in which Austria does not position itself as well as we should expect. Reform of Austrian democracy should therefore focus more intensively on these "hot spot" topics and fields of policy application (on the financing of politics and political parties in Austria, see, e.g., Sickinger 2009).
3. *Balancing of political power*: For Western Europe, Wolfgang C. Müller and Kaare Strøm (2000, p. 589) empirically enumerated and calculated the higher-risk ruling parties which are exposed to in upcoming elections of losing, rather than maintaining their share of votes. That would, therefore, be a manifestation of the phenomenon of *government/opposition cycles* and of *political swings* (*left/right swings*) that occur regularly in democracies. A particular feature of the Austrian national parliament ("*Nationalrat*") is the existence of a "right" mandate majority of center-right and right-wing parties since the parliamentary election of 1983. Conversely, it can be argued that possibly in reaction to the conservative federal governments (in coalition arrangements of ÖVP/FPÖ and ÖVP/BZÖ parties), on the federal level during the years 2000–2007, for the first time ever a "left" majority at the sub-federal provincial level resulted after 2005, when the political party composition of the nine provincial parliaments ("*Landtage*") is being aggregated together and also is being weighted on the basis of population in these provinces (Campbell 2007, pp. 392–393). For an analysis of the Austrian

federal governments in these respective years, see furthermore Wineroither (2009). The current continuation of grand center coalitions of the center-left social democrats (SPÖ) and the center-right conservatives (ÖVP) on the federal level suggests perhaps a starting erosion of the combined left majorities at the provincial level. For an improved political balance of power, the possibilities and recommendations are increased application of term limits to political office (also for chancellors and heads of provincial governments, the governors), general elimination of automatic proportional representation of political parties in provincial governments based on the number of their mandates in the provincial parliaments (called in Austria *"Proporz"*), and general introduction of direct popular elections of mayors, possibly also direct popular elections of the heads of provincial governments, i.e., the governors (paralleled by a rearrangement of the current political balance of power on provincial level) (Campbell 2007, p. 402; see also Jankowitsch 2013). For a possible reform of the electoral law, see Klaus Poier (2001) and his considerations in favor of a "minority-friendly majority representation" ("*minderheitenfreundliches Mehrheitswahlrecht*"). *The mentioned and indicated "institution of term limits" would also have had effectively prevented a phenomenon such as that of Silvio Berlusconi in Italy, where a person (with "inter-interruptions") exerted the function of Prime Minister over almost 20 years* (http://en.wikipedia.org/wiki/Silvio_Berlusconi). There also could and can be "Berlusconi" phenomena in other (Western) democracies, especially when there is no institutionalization and implementation of term limits.

4. *Referendums*: Should a public petition with a minimum number of signatures automatically be subjected to a referendum? (Should the parliament, with a "qualified majority," be able to object to it?) The following points speak against an increased application of referendums: politics (political cycles) would be too short-lived, blockade of further EU integration processes with an interest in deepening the European Union (by scapegoating EU policies at the national level), and a populist abuse of certain political themes (e.g., against immigrants). However, the fact that the national population or the voters would have the power to put forward a topic on the political agenda which may otherwise would be ignored by the ruling parties (or the parties in parliament), is a point that speaks in favor for the increased application of referendums. Therefore, the specific setting of a minimum number of signatures for a public petition would be an important decision. Two hundred fifty thousand signatures would probably not suffice. Six hundred forty thousand signatures (around 10% of the voters in Austria) perhaps may be sufficient. This reference bar could also be raised higher though, for example, to 25% of the voters (Campbell 2002, p. 39). In variation of this, there also could be a direct democracy design, where every public petition with a required minimum number of supporters would not be linked to a "binding" referendum (*Volksabstimmung*) but only to a "non-binding" or consultative referendum for advisory functions (*Volksbefragung*). More generally speaking, direct democracy approaches are possible at the national (federal) level in Austria, however, also at the subnational (regional) levels of the Austrian political system.

5. *Political education (civic education)*: In the Austrian education system (for instance, the secondary school), political education (civic education) should be introduced comprehensively and uniformly as a distinct subject ("*Unterrichtsgegenstand*"). Political education would therefore let itself conceive as a form of "democratic education" and may be reconceptualized as a "democracy education" (as well as be renamed this way?).
6. *"Democratic Audit" of Austria*: The political system of Austria, its democracy and quality of democracy, have so far not undergone a systematic *democratic audit*. Attempts of the Austrian political science community, to convince Austrian politics and Austrian politicians to support such a democratic audit of Austria, were so far not successful. For this purpose, for example, the procedure of IDEA could be used and be applied (see IDEA 2008; Beetham 1994). However, it would also be possible to hybridize or pool different procedures (for the interesting example of a performed democratic audit in Costa Rica, see Cullell 2004).

Epilogue on Cyber-Democracy

Advanced democracies or democracies of a high quality are also a "knowledge democracy." One underlying understanding here is that knowledge, knowledge creation, knowledge production, and knowledge application (innovation) behave as crucial drivers for enhancing democracy, society, and the economy. **"Cyber-democracy" = a manifestation of knowledge democracy**, where IT (information technology) and ICT (information and communications technology) matter. *However, cyber-democracy is more than an IT (ICT) concept*. "Cyber-democracy" is to look at a knowledge democracy from the perspective of a globally evolving knowledge society and knowledge economy in configurations of a multilevel architecture (top-down from global to transnational, supranational, national, subnational, and local).

The research question of our analysis focused on conceptualizing and measuring quality of democracy in international and global context. In particular, we put the two country-based democracies of the United States and of Austria into comparison. The OECD countries served as the general frame of reference for context. *Now, how does cyber-democracy relate to democracy and the quality of democracy?* In our opinion, this represents a new and challenging field, which requires further elaboration. *The evolution of cyber-democracy still is at the very beginning.* There are all the potentials for surprises in the flow of the coming events. In the following, we want to present a few propositions on cyber-democracy and the tendencies that are possibly involved and may unfold. These propositions we want to suggest as reference points for further discussions and discourses on cyber-democracy:

1. *Cyber-Democracy and Knowledge Democracy*: The progress of advanced economies and of quality of democracy depends on knowledge economy, knowledge society and knowledge democracy, their coevolution, and their mutual interlinkages (Carayannis and Campbell 2009, 2010, 2012; Campbell and

Carayannis 2013b). The transformation and shift has been from a knowledge-based economy and society directly to a knowledge economy and knowledge society. Pluralism and heterogeneity are crucial and decisive for progressing quality of democracy. The analogy to knowledge is that advanced knowledge systems are also characterized by a pluralism, diversity, and heterogeneity of different knowledge paradigms and innovation paradigms that drive in coevolution the interaction and relationship of competition, cooperation, and learning processes. *Cyber-democracy, in fact, amplifies and accelerates the momentum of knowledge democracy. Cyber-democracy is connected to democracy by building and by forming IT-based infrastructures and public spaces, where IT (information technology) helps in creating new types and new qualities of public space*. The concept and model of the "Quadruple Helix innovation system" (Carayannis and Campbell 2009, 2012) identifies the "media-based and culture-based public" (in addition to "civil society") as the one crucial helix or context for carrying on and advancing knowledge production and innovation. Therefore, in these aspects, the cyber-democracy and knowledge democracy overlap in a conceptual understanding but also in the manifestation of empirical phenomena. Cyber-democracy expresses a particular vision, for how knowledge democracy may evolve further in certain and particular characteristics. *IT-based public spaces in cyber-democracy operate nationally and subnationally. Cyber-democracy, however, also transcends the boundaries of the nation state, as such adding to the building of a transnational, in fact global, public space*. Public spaces in cyber-democracy are certainly multilevel (global, national, and subnational). The global and transnational aspect of public space in cyber-democracy certainly represents this one very new and radical aspect, allowing for a global spreading of knowledge and of high-quality knowledge, in this case enabling continuous flows of knowledge and discourses beyond the limits of the nation state.

2. *Cyber-Democracy and Governance*: Cyber-democracy appears to have several implications for governance of democracy and governance in democracy, also e-governance in e-democracy (Kneuer 2016). In an etymological understanding, the origin of the word "governance" refers back to ancient Greek (the verb *kybernein* or κυβερνειν infinitive, *kybernao* or κυβερνάω first person), where the literal meaning was to steer or to guide a vehicle that was land-based or sea-based (a ship), but Plato already emphasized the idea of governance of men or people. The prefix "cyber" thus explicitly reflects the etymological component of "steering" (Campbell and Carayannis 2013b, p. 3). Based on this assignment, we could paraphrase "cybernetics" as a science of steering. Cybernetics refers to feedback and focuses on regulatory systems, but of course there exist different approaches to cybernetics (Wiener 1948; Kuhn 1962; Umpleby 1990). *Cyber-democracy, therefore, may be understood as a governance of democracy in context of knowledge democracy. This governance can be interested and motivated to use (also to use) new IT-based infrastructures (e.g., the Internet or web) and public spaces for purposes of governance. Furthermore, public spaces (advanced public spaces) also define references for quality of governance in democracy.*

3. *Cyber-Democracy, Global Democracy, and Global Society*: The concept of "global democracy" can take different meanings. Global democracy could be translated into regimes and systems of intergovernmental cooperation or supranational integration. This implies to tie global democracy directly to mechanisms of government and governance. Alternatively, we may want to think of global democracy more in terms of an evolving (self-evolving) of a *global society. Particularly the features of an international knowledge flow and of IT-based infrastructures (and of public spaces), which clearly transcend the borders and boundaries of nation states, support the notions of a global society, where, at least partially, the global society even bypasses the nation state*. In that scenario, the global society would develop vis-à-vis the traditional nation state. One consequence of this is that nation states do not have the power anymore of controlling or suppressing successfully the global flow of knowledge. The serial breakdown of authoritarian (totalitarian) political regimes during the course of the Arab Spring serves here as a good example (Xavier and Campbell 2014, 2017). But of course, also the concept of *global society* would have to be translated into a multilevel architecture of arrangements, distinguishing between global, national and subnational levels within context of the *global society* (global knowledge society).
4. *Cyber-Democracy and the New Rights and New Freedoms*: Cyber-democracy provides governments in democracies (and in nondemocracies) with additional IT-based technical means and capabilities of monitoring the flow of knowledge on the Internet. *But of course, not everything, which is technically possible, is also feasible in terms of democracy and quality of democracy. This creates a need of restricting (technically possible) monitoring activities of democratic governments. Democratic governments, in fact, should impose on themselves also self-restrictions in that respect*. A related question here is: Is it proper for democratic governments to "spy" against each other? Where is here the line to be drawn? For example, does an e-mail qualify, in a legal sense, as a "postcard" or as a "letter"? *It is obvious that cyber-democracy requires a debate and discourse on the New Rights and New Freedoms of citizens in context of knowledge democracy, protecting citizens against monitoring activities of their governments that are at conflict with principles of quality of democracy.*

Cross-References

- ▶ Academic Firm in Cyber-Development: The New Design and Redesign Proposition for Entrepreneurship in the Innovation-Driven Knowledge Economy
- ▶ Citizenship Education and New Media: Opportunities and Challenges
- ▶ Cyber-Democracy in the Middle East
- ▶ Epistemic Governance and Epistemic Innovation Policy in Higher Education for Cyber-Development
- ▶ Libya: Where Cyber-Democracy Reached Its Limits – How the Case of Libya Challenges the Idea of Cyber-Development

► Quadruple and Quintuple Helix Innovation Systems and Mode 3 Knowledge Production

References

Barth, T. D. (2010). *Konzeption, Messung und Rating der Demokratiequalität. Brasilien, Südafrika, Australien und die Russische Föderation 1997–2006*. Saarbrücken: VDM Verlag Dr. Müller.

Barth, T. D. (2011). *Die 20 besten Demokratien der Welt. Freiheit – Gleichheit – Demokratiequalität auf einen Blick*. Norderstedt: Books on Demand.

Bast, G., Carayannis, E. G., & Campbell, D. F. J. (Eds.). (2015). *Arts, research, innovation and society*. New York: Springer. http://www.springer.com/business+%26+management/technology+management/book/978-3-319-09908-8.

Beck, E. R. A., & Schaller, C. (2003). *Zur Qualität der britischen und österreichischen Demokratie*. Vienna: Böhlau.

Beetham, D. (1994). Key principles and indices for a democratic audit. In D. Beetham (Ed.), *Defining and measuring democracy* (pp. 25–43). London: Sage.

Beetham, D. (2004). Freedom as the foundation. *Journal of Democracy, 15*(4), 61–75.

Beetham, D., Byrne, I., Ngan, P., & Weir, S. (2002). *Democracy under Blair. A democratic audit of the United Kingdom*. London: Politico's Publishing.

Bühlmann, M., Merkel, W., Müller, L., & Weßels, B. (2011). The democracy barometer: A new instrument to measure the quality of democracy and its potential for comparative research. *European Political Science*. https://doi.org/10.1057/eps.2011.46. http://www.palgrave-journals.com/eps/journal/vaop/ncurrent/abs/eps201146a.html.

Campbell, D. F. J. (2002). Zur Demokratiequalität von politischem Wechsel, Wettbewerb und politischem System in Österreich. In D. F. J. Campbell & C. Schaller (Eds.), *Demokratiequalität in Österreich* (pp. 19–46). Opladen: Leske + Budrich. http://www.oegpw.at/sek_agora/publikationen.htm and http://www.ssoar.info/ssoar/View/?resid=12473.

Campbell, D. F. J. (2007). Wie links oder wie rechts sind Österreichs Länder? Eine komparative Langzeitanalyse des parlamentarischen Mehrebenensystems Österreichs (1945–2007). *SWS-Rundschau, 47*(4), 381–404. http://www.sws-rundschau.at/archiv/SWS_2007_4_campbell.pdf and http://www.ssoar.info/ssoar/View/?resid=12472&lang=de.

Campbell, D. F. J. (2008). *The basic concept for the democracy ranking of the quality of democracy*. Vienna: Democracy Ranking. http://www.democracyranking.org/downloads/basic_concept_democracy_ranking_2008_A4.pdf.

Campbell, D. F. J. (2011). *Key findings (summary abstract) of the democracy ranking 2011 and of the democracy improvement ranking 2011*. Vienna: Democracy Ranking. http://www.democracyranking.org/downloads/Key-findings_Democracy-Ranking_2011_en-A4.pdf.

Campbell, D. F. J. (2012). Die österreichische Demokratiequalität in Perspektive [The quality of democracy in Austria in perspective]. In L. Helms & D. M. Wineroither (Eds.), *Die österreichische Demokratie im Vergleich [Austrian democracy in comparison]* (pp. 293–315). Baden-Baden: Nomos.

Campbell, D. F. J. (2013). *Conceptualizing and measuring the quality of democracy in global comparison. Freedom, equality, sustainable development, and political self-organization (political swings, government/opposition cycles) in 151 countries (democracies, semi-democracies and non-democracies), 2002–2008. Habilitation treatise ("Habilitationsschrift")*. Vienna: University of Vienna.

Campbell, D. F. J. (2015a). Reformvorschläge für Österreichs Demokratie: Diskussionspunkte zur Demokratiequalität [Reform proposal for Austrian democracy: Discussion points on quality of democracy]. In T. Öhlinger & K. Poier (Eds.), *Direkte Demokratie und Parlamentarismus. Wie kommen wir zu den besten Entscheidungen? [Direct democracy and parliamentarism. How do we make the best decisions?]* (pp. 43–56). Vienna: Böhlau. http://www.amazon.de/Direkte-

Demokratie-Parlamentarismus-kommen-Entscheidungen/dp/3205796659/ref=sr_1_1?ie=UTF8&qid=1423650423&sr=8-1&keywords=klaus+poier.

Campbell, D. F. J. (2015b). Verbesserungsmöglichkeiten und Reformvorschläge für Demokratiequalität in Österreich. [Possibilities for improving and reforming quality of democracy in Austria]. *SWS-Rundschau [Social Scientific Review], 55*(2), 219–239. ISSN: 1013-1469. http://www.sws-rundschau.at/html/archiv_abstract.php?language=de&id=328&heft=82.

Campbell, D. F. J. (2017). Die österreichische Demokratiequalität in Perspektive [The quality of democracy in Austria in perspective]. In L. Helms & D. M. Wineroither (Eds.), *Die österreichische Demokratie im Vergleich [Austrian democracy in comparison]* (pp. 365–393). Baden-Baden: Nomos. https://www.amazon.de/%C3%B6sterreichische-Demokratie-Vergleich-Politik-Kleineren/dp/384873124X/ref=sr_1_3?s=books&ie=UTF8&qid=1504590230&sr=1-3&keywords=die+%C3%B6sterreichische+demokratie+im+vergleich.

Campbell, D. F. J., & Barth, T. D. (2009). Wie können Demokratie und Demokratiequalität gemessen werden? Modelle, Demokratie-Indices und Länderbeispiele im globalen Vergleich. *SWS-Rundschau, 49*(2), 208–233. http://www.sws-rundschau.at/archiv/SWS_2009_2_Campbell.pdf and http://www.ssoar.info/ssoar/View/?resid=12471.

Campbell, D. F. J., & Carayannis, E. G. (2013a). Quality of democracy and innovation. In E. G. Carayannis, I. N. Dubina, N. Seel, D. F. J. Campbell, & D. Uzunidis (Eds.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 1527–1534). New York: Springer. http://link.springer.com/referenceworkentry/10.1007%2F978-1-4614-3858-8_509#.

Campbell, D. F. J., & Carayannis, E. G. (2013b). *Epistemic governance in higher education. Quality enhancement of universities for development* (SpringerBriefs in Business). New York: Springer. http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6.

Campbell, D. F. J., & Carayannis, E. G. (2014). Explaining and comparing quality of democracy in quadruple helix structures: The quality of democracy in the United States and in Austria, challenges and opportunities for development. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 117–148). New York: Springer. https://link.springer.com/chapter/10.1007/978-1-4939-1028-1_4 and http://www.springer.com/de/book/9781493910274.

Campbell, D. F. J., & Carayannis, E. G. (2016). The academic firm: A new design and redesign proposition for entrepreneurship in innovation-driven knowledge economy. *Journal of Innovation and Entrepreneurship, 5*(12), 1–10. https://doi.org/10.1186/s13731-016-0040-1. http://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-016-0040-1.

Campbell, D. F. J., & Schaller, C. (Eds.). (2002). *Demokratiequalität in Österreich. Zustand und Entwicklungsperspektiven*. Opladen: Leske + Budrich. http://www.oegpw.at/sek_agora/publikationen.htm und http://www.ssoar.info/ssoar/View/?resid=12473.

Campbell, D. F. J., & Sükösd, M. (Eds.). (2002). *Feasibility study for a quality ranking of democracies*. Vienna: Global Democracy Award. http://www.democracyranking.org/downloads/feasibility_study-a4-e-01.pdf.

Campbell, D. F. J., Liebhart, K., Martinsen, R., Schaller, C., & Schedler, A. (Eds.). (1996). *Die Qualität der österreichischen Demokratie. Versuche einer Annäherung*. Vienna: Manz.

Campbell, D. F. J., Carayannis, E. G., Barth, T. D., & Campbell, G. S. (2013). Measuring democracy and the quality of democracy in a world-wide approach: Models and indices of democracy and the new findings of the "Democracy Ranking". *International Journal of Social Ecology and Sustainable Development, 4*(1), 1–16. http://www.igi-global.com/article/measuring-democracy-quality-democracy-world/77344.

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493. https://doi.org/10.1007/s13132-015-0246-7.

Campbell, D. F. J., Pölzlbauer, P., & Barth, T. D. (2017). *Democracy ranking 2016*. Vienna: Democracy Ranking Organization. http://democracyranking.org/wordpress/2016-full-dataset/.

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "Quadruple Helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46* (3/4), 201–234. http://www.inderscience.com/browse/index.php?journalID=27&year=2009&vol=46&issue=3/4 and http://www.inderscience.com/search/index.php?action=record&rec_id=23374&prevQuery=&ps=10&m=or.

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69. http://www.igi-global.com/bookstore/article.aspx?titleid=41959.

Carayannis, E. G., & Campbell, D. F. J. (2011). Open innovation diplomacy and a 21st century fractal research, education and innovation (FREIE) ecosystem: Building on the quadruple and quintuple helix innovation concepts and the "Mode 3" knowledge production system. *Journal of the Knowledge Economy, 2*(3), 327–372. http://www.springerlink.com/content/d1lr223321305579/.

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development* (SpringerBriefs in Business, Vol. 7). New York: Springer. http://www.springer.com/business+%26+management/book/978-1-4614-2061-3 and http://www.springer.com/cda/content/document/cda_downloaddocument/9781461420613-c1.pdf?SGWID=0-0-45-1263639-p174250662.

Carayannis, E. G., & Campbell, D. F. J. (2014). Developed democracies versus emerging autocracies: Arts, democracy, and innovation in quadruple helix innovation systems. *Journal of Innovation and Entrepreneurship, 3*, 12. http://www.innovation-entrepreneurship.com/content/pdf/s13731-014-0012-2.pdf and http://www.innovation-entrepreneurship.com/content/3/1/12.

Carayannis, E. G., & Campbell, D. F. J. (2015). Art and artistic research in quadruple and quintuple helix innovation systems. In G. Bast, E. G. Carayannis, & D. F. J. Campbell (Eds.), *Arts, research, innovation and society* (pp. 29–51). New York: Springer. http://link.springer.com/chapter/10.1007/978-3-319-09909-5_3.

Carayannis, E. G., Barth, T. D., & Campbell, D. F. J. (2012). The quintuple helix innovation model: Global warming as a challenge and driver for innovation. *Journal of Innovation and Entrepreneurship, 1*(1), 1–12. http://www.innovation-entrepreneurship.com/content/pdf/2192-5372-1-2.pdf.

Carayannis, E. G., Campbell, D. F. J., & Efthymiopoulos, M. P. (Eds.). (2018). *Handbook of cyber-development, cyber-democracy, and cyber-defense*. New York: Springer. http://www.springer.com/economics/policy/book/978-3-319-09068-9 and https://link.springer.com/referencework/10.1007/978-3-319-06091-0.

Cullell, J. V. (2004). Democracy and the quality of democracy. Empirical findings and methodological and theoretical issues drawn from the citizen audit of the quality of democracy in Costa Rica. In G. O'Donnell, J. V. Cullell, & O. M. Iazzetta (Eds.), *The quality of democracy. Theory and applications* (pp. 93–162). Notre Dame: University of Notre Dame Press.

Cunningham, F. (2002). *Theories of democracy.* London: Routledge.

Dahl, R. A. (1971). *Polyarchy. Participation and opposition*. New Haven: Yale University Press.

Danilda, I., Lindberg, M., & Torstensson, B.-M. (2009). Women resource centres. A Quattro Helix innovation system on the European Agenda. Paper http://www.hss09.se/own_documents/Papers/3-11%20-%20Danilda%20Lindberg%20&%20Torstensson%20-%20paper.pdf.

Democracy Ranking. (2011). *Democracy ranking 2011 and the democracy improvement ranking 2011*. Vienna: Democracy Ranking. http://www.democracyranking.org/en/ranking.htm.

Diamond, L., & Morlino, L. (2004). The quality of democracy. An overview. *Journal of Democracy, 15*(4), 20–31.

Diamond, L., & Morlino, L. (2005). *Assessing the quality of democracy.* Baltimore: The Johns Hopkins University Press.

Downs, A. (1957). *An economic theory of democracy.* Boston: Addison-Wesley.

EIU/Economist Intelligence Unit. (2010). *Democracy index 2010. Democracy in retreat*. London: Economist Intelligence Unit. http://graphics.eiu.com/PDF/Democracy_Index_2010_web.pdf.

Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation: From national systems and "Mode 2" to a triple helix of university-industry-government relations. *Research Policy, 29*, 109–123.

Freedom House. (2011a). *Freedom in the world 2011. Methodology*. Washington, DC: Freedom House. http://www.freedomhouse.org/template.cfm?page=351&ana_page=379&year=2011.

Freedom House. (2011b). *Freedom in the world – population trends*. Washington, DC: Freedom House. http://www.freedomhouse.org/images/File/fiw/historical/PopulationTrendsFIW1980-2011.pdf.

Freedom House. (2011c). *Freedom in the world aggregate and subcategory scores*. Washington, DC: Freedom House. http://www.freedomhouse.org/images/File/fiw/historical/AggregateScores_FIW2003-2011.xls.

Freedom House. (2011d). *Freedom of the press* (2011 ed, Country reports). Washington, DC: Freedom House. http://www.freedomhouse.org/template.cfm?page=107&year=2011.

Fröschl, E., Kozeluh, U., & Schaller, C. (Eds.). (2008). *Democratisation and de-democratisation in Europe? Austria, Britain, Italy, and the Czech Republic – A comparison*. Innsbruck: Studienverlag (Transaction Publishers).

Gastil, R. D. (1993). The comparative survey of freedom: Experiences and suggestions. In A. Inkeles (Ed.), *On measuring democracy* (pp. 21–46). New Brunswick: Transaction Publishers.

Geissel, B., Kneuer, M., & Lauth, H.-J. (2016). Measuring the quality of democracy: Introduction. *International Political Science Review, 37*(5), 571–579. http://journals.sagepub.com/doi/pdf/10.1177/0192512116669141.

Giebler, H., & Merkel, W. (2016). Freedom and equality in democracies: Is there a trade-off? *International Political Science Review, 37*(5), 594–605. http://journals.sagepub.com/doi/full/10.1177/0192512116642221.

Harding, S., Phillips, D., & Fogarty, M. (1986). *Contrasting values in Western Europe. Unity, diversity and change. Studies in the contemporary values of modern society*. London: MacMillan.

Hausmann, R., Tyson, L. D., & Zahidi, S. (Eds.). (2011). *The global gender gap report 2011*. Genf: World Economic Forum. http://www3.weforum.org/docs/WEF_GenderGap_Report_2011.pdf.

Held, D. (2006). *Models of democracy*. Stanford: Stanford University Press.

Helms, L. (2007). *Die Institutionalisierung der liberalen Demokratie. Deutschland im internationalen Vergleich*. Frankfurt: Campus.

Helms, L. (2016). Democracy and innovation: From institutions to agency and leadership. *Democratization, 23*(3), 459–477. http://www.tandfonline.com/doi/abs/10.1080/13510347.2014.981667.

Heritage Foundation. (2011). *2011 index of economic freedom. Ranking the countries*. Washington, DC: The Heritage Foundation. http://www.heritage.org/index/pdf/2011/Index2011_Ranking.pdf.

Huddleston, T., Niessen, J., Chaoimh, E. N., & White, E. (Eds.). (2011). *Migrant integration policy index III*. Brüssel: British Council and Migration Policy Group. http://www.mipex.eu/sites/default/files/downloads/migrant_integration_policy_index_mipexiii_2011.pdf.

IDEA/International Institute for Democracy and Electoral Assistance (David Beetham/Edzia Carvalho/Todd Landman/Stuart Weir). (2008). *Assessing the quality of democracy. A practical guide*. Stockholm: International IDEA. http://www.idea.int/publications/aqd/index.cfm.

IMF/International Monetary Fund. (2011). *World economic outlook, April 2011*. Washington, DC: International Monetary Fund. http://www.imf.org/external/pubs/ft/weo/2011/01/pdf/text.pdf.

In't Veld, & Roeland, J. (Eds.). (2010). *Knowledge democracy. Consequences for science, politics, and media*. Heidelberg: Springer. http://www.springer.com/de/book/9783642113802 and https://link.springer.com/book/10.1007%2F978-3-642-11381-9.

Jankowitsch, R. M. (2013). *Tretet zurück! Das Ende der Aussitzer und Sesselkleber*. Wien: Verlag Carl Ueberreuter.

Kneuer, M. (2016). E-democracy: A new challenge for measuring democracy. *International Political Science Review, 37*(5), 666–678. http://journals.sagepub.com/doi/full/10.1177/0192512116657677.

Kuhn, T. S. (1962). *The structure of scientific revolutions*. Chicago: The University of Chicago Press.

Lauth, H.-J. (2004). *Demokratie und Demokratiemessung. Eine konzeptionelle Grundlegung für den interkulturellen Vergleich*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Lauth, H.-J. (2010). Möglichkeiten und Grenzen der Demokratiemessung. *Zeitschrift für Staats- und Europawissenschaften, 8*(4), 498–529.

Lauth, H.-J. (2011). Qualitative Ansätze der Demokratiemessung. *Zeitschrift für Staats- und Europawissenschaften, 9*(1), 49–77.

Lauth, H.-J. (2016). The internal relationships of the dimensions of democracy: The relevance of trade-offs for measuring the quality of democracy. *International Political Science Review, 37*(5), 606–617. http://journals.sagepub.com/doi/full/10.1177/0192512116667630.

Lauth, H.-J., Pickel, G., & Welzel, C. (Eds.). (2000). *Demokratiemessung*. Wiesbaden: Westdeutscher Verlag.

Marshall, T. H. (1964). *Class, citizenship, and social development. Essays*. Garden City: Doubleday.

Morlino, L., & Quaranta, M. (2016). What is the impact of the economic crisis on democracy? Evidence from Europa. *International Political Science Review, 37*(5), 618–633. http://journals.sagepub.com/doi/full/10.1177/0192512116639747.

Müller, W. C., & Strøm, K. (2000). Conclusion: Coalition governance in Western Europe. In W. C. Müller & K. Strøm (Eds.), *Coalition governments in Western Europe* (pp. 559–592). Oxford: Oxford University Press.

Munck, G. L. (2009). *Measuring democracy*. Baltimore: The Johns Hopkins University Press.

Munck, G. L. (2014). What is democracy? A reconceptualization of the quality of democracy. Political concepts: Committee on Concepts and Methods. Working Paper Series (Working Paper 60, May 2014). http://www.concepts-methods.org/Files/WorkingPaper/60%20Munck%20(2014).pdf.

O'Donnell, G. (2004a). Human development, human rights, and democracy. In G. O'Donnell, J. V. Cullell, & O. M. Iazzetta (Eds.), *The quality of democracy. Theory and applications* (pp. 9–92). Notre Dame: University of Notre Dame Press.

O'Donnell, G. (2004b). Why the rule of law matters. *Journal of Democracy, 15*(4), 32–46.

OECD. (2011). *OECD.Stat extracts. Social and welfare statistics*. Paris: OECD. http://stats.oecd.org/index.aspx.

Pelinka, A. (2008). Democratisation and de-democratisation in Austria. In E. Fröschl et al. (Eds.), *Democratisation and de-democratisation in Europe? Austria, Britain, Italy, and the Czech Republic – A comparison* (pp. 21–36). Innsbruck: Studienverlag (Transaction Publishers).

Pelinka, A., & Rosenberger, S. (2003). *Österreichische Politik. Grundlagen, Strukturen, Trends*. Vienna: Facultas WUV.

Pickel, S., & Pickel, G. (2006). *Politische Kultur- und Demokratieforschung. Grundbegriffe, Theorien, Methoden*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Poier, K. (2001). *Minderheitenfreundliches Mehrheitswahlrecht. Rechts- und politikwissenschaftliche Überlegungen zu Fragen des Wahlrechts und der Wahlsystematik*. Vienna: Böhlau.

Przeworski, A., Alvarez, M. E., Cheibub, J. A., & Limongi, F. (2003). *Democracy and development. Political institutions and well-being in the world, 1950–1990*. Cambridge: Cambridge University Press.

Rosenberger, S. (Ed.). (2010). *Asylpolitik in Österreich. Unterbringung im Fokus*. Vienna: Facultas.

Rosenberger, S., & Seeber, G. (2008). *Wählen*. Vienna: Facultas WUV (UTB).

Schedler, A. (2006). *Electoral authoritarianism: The dynamics of unfree competition*. Boulder: L. Rienner Publishers.

Schmidt, M. G. (2010). *Demokratietheorien*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Schmitter, P. C. (2004). The ambiguous virtues of accountability. *Journal of Democracy, 15*(4), 47–60.

Sickinger, H. (2009). *Politikfinanzierung in Österreich*. Vienna: Czernin.

Sodaro, M. J. (2004). *Comparative politics. A global introduction*. Boston: McGraw Hill.

Stoiber, M. (2011). *Die Qualität von Demokratien im Vergleich. Zur Bedeutung des Kontextes in der empirisch vergleichenden Demokratietheorie*. Baden-Baden: Nomos.

TI/Transparency International. (2011). *Transparency international annual report 2010*. Berlin: TI. http://www.transparency.org/content/download/61964/992803.

Umpleby, S. A. (1990). The science of cybernetics and the cybernetics of science. *Cybernetics and Systems, 21*(1), 109–121. ftp://ftp.vub.ac.be/pub/projects/Principia_Cybernetica/Papers_Umpleby/Science-Cybernetics.txt.

UNDP/United Nations Development Program. (2000). *Human development report 2000. Human rights and human development*. Oxford: Oxford University Press. http://hdr.undp.org/en/reports/global/hdr2000/.

UNDP/United Nations Development Program. (2011). *Human development report 2011. Sustainability and equity: A better future for all*. New York: UNDP. http://hdr.undp.org/en/media/HDR_2011_EN_Complete.pdf.

Valchars, G. (2006). *Defizitäre Demokratie. Staatsbürgerschaft und Wahlrecht im Einwanderungsland Österreich*. Vienna: Braumüller.

Vanhanen, T. (2000). A new dataset for measuring democracy, 1810–1998. *Journal of Peace Research, 37*(2), 251–265.

Wiener, N. (1948). *Cybernetics or control and communication in the animal and the machine*. New York: Wiley.

Wineroither, D. M. (2009). *Kanzlermacht – Machtkanzler? Die Regierung Schüssel in historischen und internationalen Vergleich*. Vienna: LIT-Verlag.

Winiwarter, V., & Knoll, M. (2007). *Umweltgeschichte*. Cologne: Böhlau.

Xavier, R. F., & Campbell, D. F. J. (2014). The effects of cyberdemocracy on the Middle East: Egypt and Iran. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 147–173). New York: Springer. http://link.springer.com/chapter/10.1007/978-1-4939-1028-1_5.

Xavier, R. F., & Campbell, D. F. J. (2017). Cyber-democracy in the Middle East. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Handbook of cyber-development, cyber-democracy, and cyber-defense* (pp. 1–30). New York: Springer. https://link.springer.com/referenceworkentry/10.1007/978-3-319-06091-0_5-1.

The Quality of Democracy as a Key to Cyber-Democracy

19

Thorsten D. Barth and Willi Schlegelmilch

Contents

Abstract

Never until now during the known history of mankind was it so easy to communicate globally and to share information so rapidly. An increase of information and knowledge is resulting from the growing information exchange. The technical transformation processes have the impact that more and more aspects of politics, policies, or public opinion formation in a democracy are already now and will further be transferred into the digital world. A variety of factors is contributing to and responsible for these transformation processes. In this context, global networking and communication can be seen as one of the most critical factors. The increasing global networking and communication is closely linked to and build upon revolutionary developments in the information technology. Having this in mind, it becomes clear that today's democratic societies have to be modernized, if they want to survive as functioning political democratic systems in

T. D. Barth (✉)
Political Scientist and Academic Entrepreneur, Vienna Democracy Ranking Organization – Academic Ranking Team, Vienna, Austria
e-mail: thorsten.d.barth@gmail.com

W. Schlegelmilch
Accounting System Standardisation, Schönaich, Germany
e-mail: cwschlegelmilch@t-online.de

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_44

the already established digital environment. This is even more important in the digital era for a democracy's future as a Cyber Democracy. The thesis of this chapter is that a Cyber Democracy can only be implemented and maintained sustainably, when the basic principles of a democracy as well as the quality standards of a high-quality democracy are fulfilled to an extremely high degree. Our conclusion is that in due consideration of the high-quality standards for a democracy, a basic and sustainable concept for a Cyber Democracy can be established in the digital world.

Keywords
Quality of democracy · Democracy · Cyber democracy · Information

Introduction

Never until now during the known history of mankind was it so easy to communicate globally and to share information so rapidly. An increase of information and knowledge is resulting from the growing information exchange. The technical transformation processes have the impact that more and more aspects of politics, policies, or public opinion formation in a democracy are already now and will further be transferred into the digital world. A variety of factors is contributing to and responsible for these transformation processes. In this context, global networking and communication can be seen as one of the most critical factors. The increasing global networking and communication is closely linked to and builds upon revolutionary developments in the information technology. Having this in mind it becomes clear that democratic societies have to be modernized for being capable of surviving as functioning political democratic systems in the already established digital environment. This is even more important in the digital era for having a future as a Cyber Democracy.

Many concepts for democracies aim in the context of technical developments at further developing the existing democracy into a democracy into the Cyber Space or even establishing a Cyber Democracy. Through better and better technical standards, the concepts for a Cyber Democracy appear to be plausible and sustainable, but the Cyber Democracy also comprises implications that can deeply endanger an existing democracy. For transforming the idea of a Cyber Democracy into a sustainable democratic system the highest democratic quality standards must be fulfilled by the existing democracy. With this chapter we represent the thesis that a Cyber Democracy can only be established and sustainably maintained, when the basic principles for a democracy are met to an extremely high degree as well as the quality standards for a high-quality democracy: "High-quality democracy as a key to Cyber Democracy."

The chapter shows based on basic underlying democracy theories (see Barth 2013; Barth and Schlegelmilch 2014) what democracy means, what determines the quality of a democracy, and which forming characteristics of democratic quality can be found in the real world. Based on the democracy measurement, we outline what Cyber Democracy is and which implications Cyber Democracy has on a democratic system (see Barth and Schlegelmilch 2014). Our conclusion is that under

consideration of the highest quality standards for a democracy, the foundation for a basic and sustainable concept of democracy in the digital world can be established.

Democracy and Measuring the Quality of Democracy

As prerequisite for a discussion about Cyber Democracy as a sustainable form of a modern democracy, we must define (see Barth and Schlegelmilch 2014; Barth 2013) what is meant with democracy and what can be understood as the quality of a democracy. It is also necessary to understand which quality of democracies is currently existing in the real world.

Democracy and the Quality of Democracy

Even if the term "democracy" is very often used in the political and every day communication as well as in the media, it is perceived differently in the political sciences: Despite of a long lasting history of ideas, there are still quite different interpretations and views about what actually can be understood as democracy. Fundamentally for this chapter and following Abraham Lincoln, democracy shall be understood as "government of the people, by the people, and for the people" (Lincoln 1863, quote from Lincoln and Chittenden, 2009/1908, p. 133). Lincoln's definition of democracy is old and it seems simple, but it describes accurately the meaning of democracy. What is therefore a democracy in terms of the people? To regard a democracy in terms of the people means to focus on the aspect of the "quality of democracy" (see O'Donnell 2004, pp. 9–10). Whereas in earlier research about democracy the main question was whether democracy is existing in a country or not (see Dahl 1971, pp. 248–249), the latest research about democracy is focused on the question which quality is really provided by a democracy? (see Campbell and Barth 2009, p. 210).

The subject of determining the "quality of a democracy" has gained much more relevance in the democracy research during the recent years (see, e.g., Campbell and Barth 2009; Diamond and Morlino 2005; Barth 2011) (The new study of democratic quality is important, because the quality of democracy and a sustainable development are closely linked in a Quintuple Helix Model: It means that a high-quality democracy can be seen as a prerequisite to promote knowledge, sustainability and innovation in a democracy (see Carayannis and Campbell 2010, pp. 58–62; Barth 2011, pp. 4–7).) Despite the disagreements about the definitions for and the determination of democratic quality and even with accepting the existing variety of democratic systems, a country is considered democratic, when the following fundamental criteria are fulfilled (see, e.g., Campbell and Barth 2009, Barth 2013; Diamond and Morlino 2005): There is a Demos (= the people) taking or supporting political decisions through elections or polls. The public is the confident bearer of the government (= public sovereignty) and has chosen (= e.g., through a constitution) a political system (= constitutional power). In addition there is a territory (= the national territory), within which the decisions taken are applied. Last but

not least, it is a fundamental criterion of a democracy that a selected government can be changed following repeating and bindingly defined procedures. In a representative democracy, the representatives are selected in order to execute sovereignty. In a direct democratic system, the public is directly taking decisions, e.g., through a referendum or through cooperative planning for complex factual issues. In addition, a democracy guarantees basic rights, e.g., civil liberties and fundamental freedom, e.g., religious liberty to everybody as against every other single person, as against the state, and as against the various interest groups of the society. A democracy is furthermore especially characterized through the existing freedom of opinion, the freedom of the press and the freedom of radio broadcasting as well as it is offering the people a separation of powers between the three organs of the state: The legislation (the parliament), the executive authority (the government), and the judiciary (the legal power). During elections in representative democracies or during a voting in direct democracies, the following democratic minimum guidelines and minimum standards must also be fulfilled:

1. General election: Everybody holding a voting right can participate at elections and polls (active right to vote) and also owns a passive right to vote
2. Free election: There is no pressure in any form applied to the people holding a right to vote
3. Equal election: Any eligible voter has the same quantity of votes
4. Direct election: During a voting for specific persons, the given votes are directly accounted to these candidates
5. Secret election: To ensure freedom of choice, the election should be done secretly and the eligible voters should have sufficient time for taking their decision

Now the question needs to be raised: whether Lincoln's concept of democracy is still used today or is already forgotten in democracies? In recent years, as Taureck describes, a change to the concept of Abraham Lincoln has been established (see Taureck 2010, pp. 16–17): If we talk about democracy today all is about a democracy with the elements "of the people" and "for the people," but the important meaning of "by the people" seems to be lost (ibid.). This finding is alarming, because it means democracy is losing their base ("by the people") in times of crises, globalization, etc. (see Fröschl et al. 2008). Hence, if the meaning of "by the people" falls in the background, it is necessary to analyze what is happening in democracies and finally to ask what the quality of democracy is? (see Campbell 2008; Campbell and Barth 2009; Bühlmann et al. 2008a; Barth 2010): "Contemporary democracy hardly is by the people; but it certainly is of the people and, because of this, it should also be for the people" (O'Donnell 2005, p. 9).

Measuring the Quality of Democracy in the World

Measuring the quality of democracy means to carry out a quality management about democracy. On the one hand quality management improves the quality of democracies and on the other hand it saves the quality of democracies. However, we can only

improve or save democracies when knowing where we stood yesterday and where we stand today. With the aim of measuring the quality of democracy, political science is trying to restore Lincoln's original definition of democracy (see Bühlmann et al. 2008b; Barth 2010). Today democracy provides eight dimensions of a quality product, say Diamond and Morlino (see 2005, pp. xiv–xxxi):

1. "rule of law,"
2. "vertical accountability,"
3. "horizontal accountability,"
4. "participation,"
5. "competition,"
6. "freedom,"
7. "equality" and
8. "responsibility."

At the same time, democracy should not be regarded as a political system only: In terms of quality, democracy describes a total product of the development of a society (see O'Donnell 2004; Campbell 2008; Carayannis and Campbell 2009, 2010). We have to understand that today's democracy is a product of "human rights" and "human development" (O'Donnell 2004, p. 10). Also economic development is part of our democracy (see Macpherson 1973, p. 25; Lipset 1960; Rueschemeyer et al. 1992). A special focus in the theory of the quality of democracy deals with the lived democratic content a democracy gives to its citizens: The search for the content of a democracy is the search for the values of freedom and equality (see Diamond and Morlino 2005, p. xxv; Pelinka 2008, p. 21). Freedom and equality are the substance and the tension for a today's liberal democracy (see Diamond and Morlino 2005, pp. xxv–xxix). Freedom and equality are the two crucial features of today's democracies because both values determine how democracy will develop politically, economically, and socially. In established democracies with a welfare state the question is which balance between the economic aspects of freedom and the social aspects of equality should be sought in times of crisis and in the transformation to the digital world? Basically the goal could be clear: Freedom and equality should be developed in a way, so that they can strengthen democracy and promote the quality of a democracy.

Today's democracy is the design of our current form of *high-quality democracy* and it is the expression of our quality of life, prosperity, "innovation, knowledge and know-how" (Barth 2011, p. 2; Carayannis et al. 2012). Therefore, the new research on democracy and its quality shows an annual status for democracies in form of ratings (see Barth 2010; Barth 2013) or in form of rankings (see Campbell et al. 2014; NCCR 2011).

For the discussion of the implications of a Cyber Democracy, we therefore want to give an empirical overview about the current developments regarding the quality of democracy based on a global comparison for 2015. This comparison is based on the Democracy Ranking (Read more about the Democracy Ranking of the Quality of Democracy on: http://democracyranking.org) conducted by the independent democratic research initiative (see Figs. 1, 2, and 3; Table 1). The Democracy Ranking is

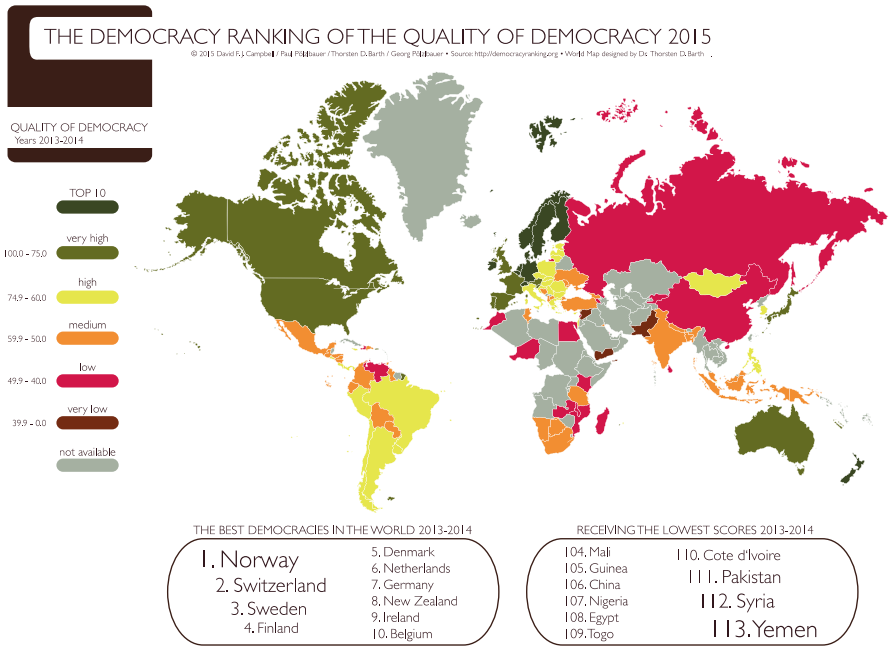


Fig. 1 World Map of the democracy ranking 2015

an annual study of democracy (Initiator of this project is Sàndor Hasenöhrl, an entrepreneur from the computer and software industry.), which is undertaking a global investigation of democracies: In this study, states are investigated, who have a population of at least 1,000,000 inhabitants and are classified by Freedom House as "free" or "partly free" (see Campbell et al. 2012) (Although the Russian Federation, Bahrain, Yemen, China, Egypt, Libya, Tunisia and Syria were classified by Freedom House as "not free," they were integrated from the year 2012 (The goal is to identify where these states are classified in respect of democracy and the quality of democracy).) The ranking is defined by the fundamental theory of democracy by Guillermo O'Donnell and regards democracy as a total product of "human rights" (as freedom) and "human development" (see O'Donnell 2004; Campbell and Barth 2009). The investigations in this annual study of democracy analyze the political system's quality and degree of democracy, the economy, the health system, the education system, and the protection of environment. The ranking is a civil society project and is created by the Vienna Democracy Ranking Association: The aim of the Association is to measure countries in a neutral and empirical way.

The figures show that when classifying the democracies in a range from *very high quality* to *very low quality* of democracy, the development of the world towards democracy will still need a substantial developmental period: The most western societies find themselves with a good or even very good level of democratic quality. However, when looking to the other countries of the world we find levels of *medium*

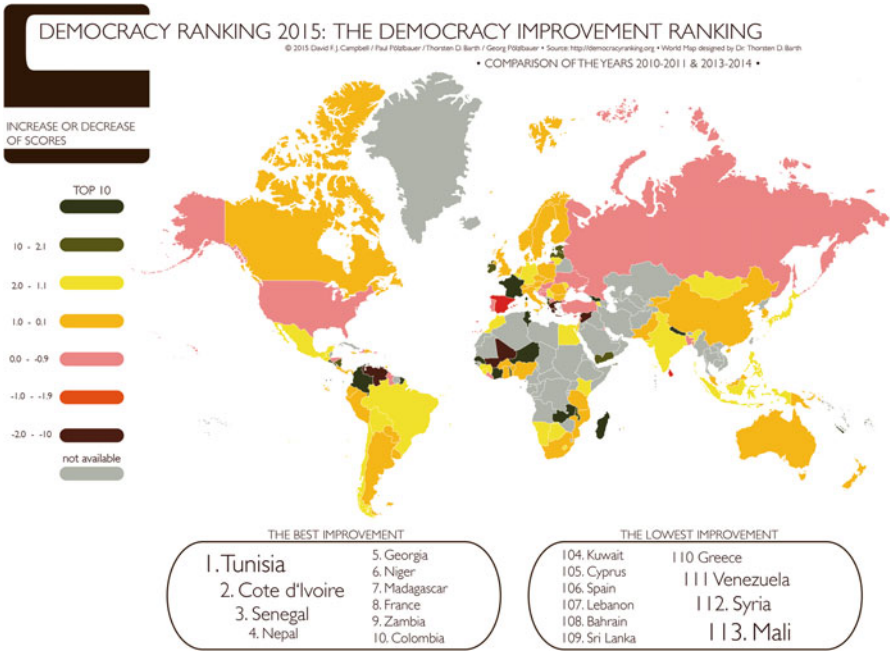


Fig. 2 World Map of the improvement of the quality of democracy: democracy ranking 2015

or *very low quality of democracy* or even quality levels of *authoritarian regimes* (see Figs. 1, 2, and 3; Table 1).

Discussion: Cyber Democracy and Its Implications for Democracy

The term "Cyber Democracy" itself contains a broad range of content and definitions. Birgit Mitterlehner describes that "cyber-democracy, e-democracy, cber-politics and e-politics are frequently used synonymously" (Mitterlehner 2014, p. 209). As a basic principle, however, Cyber Democracy comprises all the topics linked to the connections and the interconnectivity between the information technology and the processes in a democracy, e.g., for the participation of the people, the competition during elections, or the administrative processes. David Campbell (2014, p. 113) pointed out that the "ramifications" of Cyber Democracy are the following:

(1) The networking opportunities and capabilities of interaction and communication increase
(2) The volume of codified knowledge cumulates, and the possibilities to access (publicly access) this knowledge also improve

(3) Digitalized (electronic) information and knowledge, and the World-Wide Web, created a network-style fundament and infrastructure of knowledge, allowing a knowledge conversion of the local into the global (gloCal) and vice versa, resulting in a gloCal platform for communication and knowledge interaction and knowledge enhancement.

Campbell explains further that Cyber Democracy "is connected to democracy by building and by forming IT-based infrastructures and public spaces, where IT (information technology) helps in creating new types and new qualities of public space" (Campbell 2014, p. 114). Following this, Cyber Democracy can through technological instruments or the medium Internet enable the people to effectively increase their participation in the democracy and to strengthen their own civil rights. For this reason, the Cyber Democracy or other innovative ways of societal democracy design as, e.g., the E-Democracy are very often connected with technological

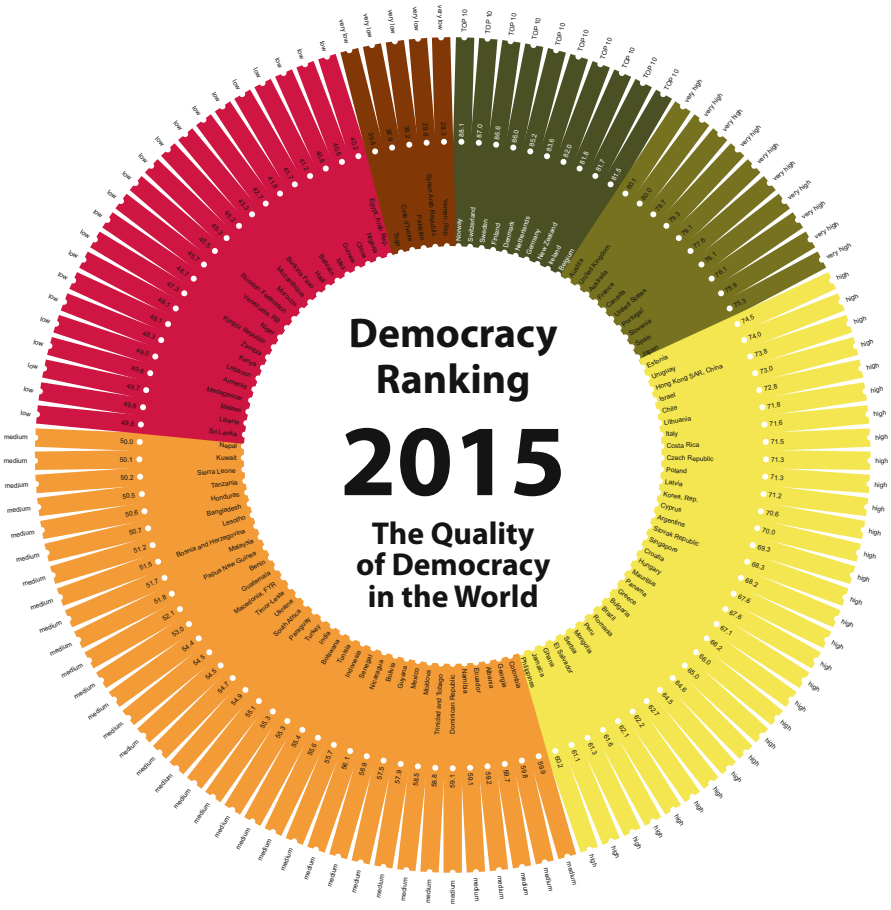


Fig. 3 The ranking of the quality of democracy 2015 (Source: http://democracyranking.org; Graphic Design based on Raw Destiny Design 2016)

Table 1 Scores of the democracy ranking 2012–2015 (covered years from 2007–2008 to 2013–2014)

Country	2007–2008	2008–2009	2009–2010	2010–2011	2011–2012	2012–2013	2013–2014
Albania	56.0	56.0	55.3	56.5	55.7	55.4	59.7
Argentina	63.3	69.1	67.2	64.0	70.2	68.5	69.3
Armenia	43.9	45.0	44.5	44.2	46.1	45.9	49.0
Australia	78.9	79.8	78.2	79.6	80.8	78.9	79.7
Austria	79.7	79.7	78.5	80.6	81.2	79.4	80.1
Bahrain	**43.2**	42.4	42.3	**40.6**	39.4	38.7	41.8
Bangladesh	42.6	47.0	48.8	48.8	49.3	49.3	50.7
Belgium	78.0	79.1	78.2	80.0	81.1	79.8	81.5
Benin	45.5	47.0	47.7	47.6	49.3	48.9	52.1
Bolivia	53.4	53.8	52.6	54.5	56.1	55.4	56.9
Bosnia and Herzegovina	48.3	49.6	48.1	48.5	50.2	49.2	51.5
Botswana	54.7	52.3	52.2	54.0	52.3	53.3	55.3
Brazil	60.4	61.1	59.6	62.3	63.8	62.8	64.6
Bulgaria	64.2	65.1	63.2	63.5	65.1	63.9	65.0
Canada	79.1	79.8	78.5	80.0	80.6	78.2	79.1
Chile	70.8	71.3	70.7	71.6	71.9	70.9	72.8
China	**36.2**	38.4	38.2	**36.9**	39.1	39.2	40.8
Colombia	55.5	55.8	54.8	56.0	57.5	58.0	59.9
Costa Rica	69.8	70.0	69.4	71.1	71.1	70.2	71.5
Croatia	67.0	67.5	66.1	67.7	68.0	66.4	67.6
Cyprus	71.4	72.0	69.7	71.8	71.5	68.9	70.0
Czech Republic	71.4	72.1	69.2	71.0	71.9	69.5	71.3
Denmark	83.8	83.9	83.4	84.1	84.4	84.8	85.2
Dominican Republic	58.7	59.4	57.1	57.6	58.9	57.9	59.1
Ecuador	57.8	58.2	57.2	57.2	57.9	57.4	59.2
Egypt, Arab Rep.	**34.8**	35.1	34.5	**37.1**	41.2	39.3	40.2

(*continued*)

Table 1 (continued)

Country	2007–2008	2008–2009	2009–2010	2010–2011	2011–2012	2012–2013	2013–2014
El Salvador	58.4	59.1	57.1	59.0	60.1	59.4	61.6
Estonia	72.5	73.3	70.6	71.6	73.2	72.6	74.5
Finland	85.8	86.0	85.2	86.3	86.7	85.5	86.0
France	77.3	77.2	74.8	76.3	78.2	77.7	79.3
Georgia	52.1	52.7	52.1	54.8	57.1	56.9	59.8
Germany	80.3	81.1	79.7	81.6	82.2	81.0	82.0
Ghana	55.9	54.0	56.3	57.5	55.5	57.2	61.3
Greece	70.2	69.9	68.2	68.5	67.5	64.3	66.0
Guatemala	48.8	50.2	49.2	49.9	51.2	51.2	53.0
Guinea	36.3	28.5	34.4	35.1	36.2	40.4	41.2
Haiti	38.1	40.3		39.7	40.2		42.7
Honduras	52.0	51.3	49.6	49.8	50.0	49.2	50.6
Hong Kong SAR, China			74.7			74.6	73.8
Hungary	70.1	70.0	66.8	67.6	68.4	66.8	67.6
India	48.7	52.3	50.8	50.1	54.1	53.1	55.3
Indonesia	50.8	52.4	51.9	52.7	54.2	53.6	55.6
Ireland	80.8	81.4	79.4	81.0	80.9	80.1	81.7
Israel	74.3	73.6	71.4	73.9	73.7	71.7	73.0
Italy	72.4	71.8	69.1	70.7	71.2	69.9	71.6
Jamaica	60.2	65.2	59.1	59.9	65.9	59.7	61.1
Japan	73.9	74.6	72.7	74.8	74.8	73.0	75.3
Kenya	40.0	41.0	42.4	42.7	44.8	46.1	48.1
Korea, Rep.	69.5	70.7	68.2	70.9	71.7	69.3	70.6
Kuwait	50.0	49.9	49.5	50.2	49.3	49.0	50.1
Kyrgyz Republic	45.5	43.8	44.0	45.7	46.4	45.7	47.3
Latvia	70.6	69.8	67.7	68.4	69.3	69.7	71.2

Lebanon	46.8	49.5	47.3	48.3	50.2	47.0	48.3
Lesotho	48.9	50.9	49.4	49.4	53.8	51.6	51.2
Liberia		49.3	49.5		52.0	51.7	49.8
Libya	**25.5**	25.9		**29.6**	38.9		
Lithuania	71.4	71.1	69.3	70.2	71.3	71.1	71.8
Macedonia, FYR	52.6	53.3	52.4	54.6	54.6	52.4	54.4
Madagascar		45.4	43.0		42.8	45.2	49.6
Malawi		44.2	45.1		47.4	48.6	49.7
Malaysia	50.6	51.3	49.2	51.5	52.0	50.1	51.7
Mauritius	64.6	65.4	65.8	65.7	66.4	66.7	67.1
Mexico	57.9	57.6	55.0	56.6	57.7	56.6	57.9
Moldova	53.4	54.4	54.0	56.7	57.8	57.1	58.5
Mongolia	56.5	58.0	59.5	58.3	59.6	61.8	62.2
Morocco	42.9	43.5	41.3	43.0	44.6	42.9	45.3
Mozambique	41.4	42.3	42.8	41.8	43.2	44.0	45.2
Namibia	52.5	53.1	53.6	53.2	54.4	56.0	59.1
Nepal	44.4	46.8	43.9	45.0	47.2	46.8	50.0
Netherlands	82.7	82.9	81.2	83.0	83.5	82.6	83.6
New Zealand	82.6	81.8	81.6	82.7	81.5	81.3	81.8
Nicaragua	53.1	52.4	52.3	53.6	53.7	54.9	56.1
Niger		39.1	38.5		43.8	46.6	46.7
Nigeria	36.3	36.8	37.0	37.4	38.7	39.9	40.6
Norway	87.3	87.4	87.4	88.5	88.3	87.8	88.1
Pakistan	33.5	37.1	35.6	37.1	38.2	35.9	38.2
Panama	63.7	64.7	63.8	65.1	65.8	64.8	66.2
Papua New Guinea		51.3	51.6		52.2	52.3	51.8
Paraguay	52.4	54.1	53.1	53.7	53.9	53.1	54.9
Peru	61.1	61.7	60.8	61.0	61.0	61.7	62.7

(*continued*)

Table 1 (continued)

Country	2007–2008	2008–2009	2009–2010	2010–2011	2011–2012	2012–2013	2013–2014
Philippines	53.9	54.0	55.6	55.8	57.3	59.2	60.2
Poland	69.2	70.3	68.9	70.5	71.1	69.7	71.3
Portugal	75.4	75.3	74.4	75.6	75.7	73.9	76.1
Romania	62.4	63.7	62.2	63.4	64.4	63.3	64.5
Russian Federation	**44.5**	45.0	43.5	**44.5**	45.8	44.4	45.5
Senegal	48.6	48.5	48.5	49.2	50.8	53.5	55.7
Serbia	59.6	60.4	58.9	60.8	61.4	60.2	62.1
Sierra Leone		44.5			47.6		50.2
Singapore	62.8	64.0	63.3	64.9	66.9	65.3	68.2
Slovak Republic	68.7	68.8	65.9	68.0	69.2	67.2	68.3
Slovenia	74.8	75.2	72.9	75.0	75.4	73.9	76.1
South Africa	53.8	55.2	52.3	53.3	55.1	53.0	54.7
Spain	77.6	77.9	76.7	77.1	76.9	74.3	75.9
Sri Lanka	51.5	52.3	51.4	49.8	49.8	48.8	49.8
Sweden	87.3	86.9	85.5	86.9	87.0	85.8	86.6
Switzerland	84.5	84.9	84.6	85.4	85.9	85.9	87.0
Syrian Arab Republic	**30.1**	31.3	35.2	**29.5**	29.2	28.3	29.8

Tanzania	45.6	43.0	45.3	48.7	47.0	48.1	50.5
Thailand	**49.7**	**51.2**	**50.1**	**51.6**	**54.2**	**54.0**	
Timor-Leste	46.2	50.4	52.1	47.3	51.3	53.2	54.5
Togo	31.9	33.4	35.8	34.6	35.8	38.3	39.8
Trinidad and Tobago	59.6	61.1	57.5	60.1	60.1	57.1	58.8
Tunisia	**37.8**	38.7	37.1	**45.8**	52.3	51.5	55.4
Turkey	53.4	53.8	51.9	53.4	54.9	53.6	55.1
Uganda		45.1	43.8		45.9	41.7	
Ukraine	56.0	57.3	54.7	54.3	54.5	52.4	54.5
United Kingdom	80.1	80.1	78.6	79.7	79.9	78.4	80.0
United States	78.3	78.7	76.7	78.5	78.8	76.9	77.6
Uruguay	71.5	72.1	71.7	72.3	73.0	72.6	74.0
Venezuela, RB	48.9	48.8	46.9	48.2	46.1	45.5	45.7
Yemen, Rep.	**25.7**	25.7	29.2	**25.9**	26.5	29.6	28.3
Zambia	37.4	39.8	40.2	41.0	44.4	44.4	48.1

Blue color: “Virtual scores” for countries, categorized by Freedom House as “not free”

innovations and the future of democracy (see Carayannis et al. 2012). Many scientists, like Ferdinand, are regarding the Cyber Democracy as a new model for the direct democracy, because it can provoke a "high degree of participation by all citizens" (Ferdinand 2003). Cyber Crimes or occurrences registered in the context of the supervision and spying of the population make out of the Cyber Democracy a very questionable democratic project for the future. Barth and Schlegelmilch (2014, pp. 200–204) explain that according to Klein et al. (1999) and from the collected literature as well as the ongoing discussions about a Cyber Democracy, the following basic points can be summarized as implications for cyber democracy (see Fig. 4):

Cyber Democracy Is Offering Cost Efficient Information for the People
In addition to offering information for the people in a cost-efficient manner, Cyber Democracy enables innovative methods and channels for transferring relevant information to the people. With the support of the new media, the people will be informed faster about the democracy and related administrative requirements. This information transfer will also be more comprehensive and very likely with an increased quality.

Cyber Democracy Needs Targeted Investments in and an Innovative Development of the New Digital Media
New digital and virtual media must be developed and implemented by the states to ensure well-informed citizens in a Cyber Democracy. A new quality of democracy will be the result as well as a new quality of people participation. The model of a Cyber Democracy appears to be highly complex and must be designed sustainably.

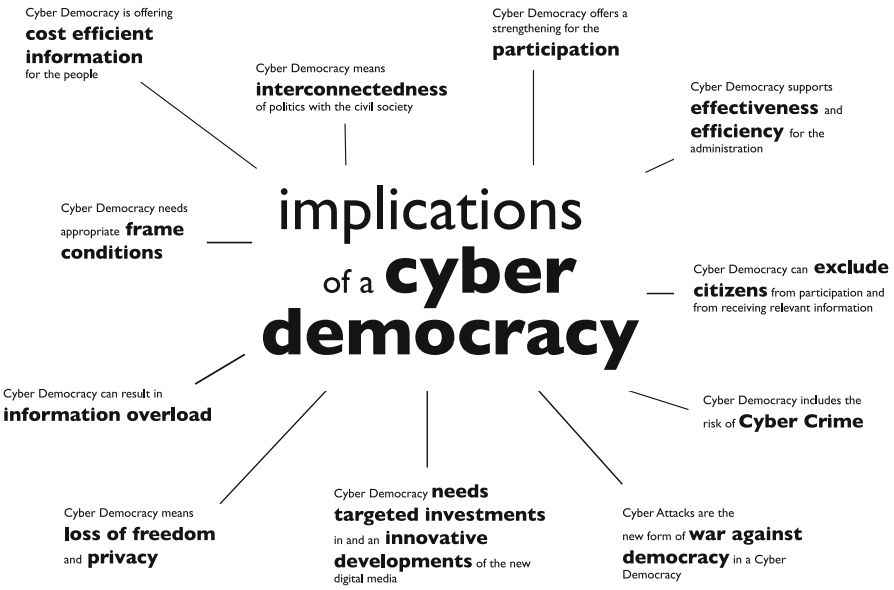


Fig. 4 Implications of a cyber democracy (Source/Graphic: Barth and Schlegelmilch 2014, p. 200)

Therefore, this implies big investments by the states willing to develop in this direction as well as necessary innovative achievements by these states.

Cyber Democracy can Result in Information Overload
It may occur in Cyber Democracies that the people will no longer be able to differentiate between important and less important democratic information. In order to avoid this to happen, new ideas for the treatment and the classification of democratic information are required, e.g., innovative forms of web design and sharing as well as presenting information. This shows on the one hand the desirable objective of the well-informed citizen and by the same token the not desired problematic picture of the overinformed and following this less-informed citizen.

Cyber Democracy Offers a Strengthening of People Participation
Cyber Democracy offers not only new chances for an increased participation of the people in the democratic processes and procedures, but also a more intensive participation in the societal and political live. Suiting examples for this increased participation would be discussion forums based on the Internet or the development of new and innovative electronic forms for elections or opinion polls. These could also be performed at any time during a day or within a defined and agreed timeframe.

Cyber Democracy can Exclude Citizens from Participation and Receiving Relevant Information
Since the idea of a Cyber Democracy is closely connected to the difficulties of getting free access to the Internet Klein et al. (1999) are using the term of the "information elites." Even if it is so, that the majority of the people in a democratic and modern society are owning devices to access the Internet especially elderly citizens and the parts of the population with less affinity to technology as such or the Internet may be excluded from the modern democracy. With a growing number of people using the Internet and increasing rates of growth for the Internet usage, a democracy therefore should not forget the remaining part of the population not able to or not even willing to be part of the Internet boom. In addition, the access to the Internet is not for free but costing money. Hence, the part of the population not being able to or willing to pay for the related Internet charges and by this remaining without online access would also stay excluded from the Cyber Democracy.

Cyber Democracy Supports Effectiveness and Efficiency for the Administration
Cyber Democracy can deliver a valuable contribution towards an effective and efficient performance of the governmental administrative machinery. Using the modern tools people can send applications or requests electronically and needed forms can be directly downloaded from the Internet. An additional advantage is the Internet-based possibility to review the status of an application or a request. Applying these possibilities will result in a faster dialogue and information exchange between the citizens and the administration, which is in addition not necessarily bound to the regular opening hours of the administration.

Cyber Democracy Includes the Risk of Cyber Crime

Together with the digitalization as well as the increasing connectivity and computer networking Cyber Crime is gaining importance and is already now a growing and profitable industry. Cyber Crime is posing a considerable danger on the democratic processes: It can indicate cases of manipulation or supervision in the Internet and goes along with the population's increasing demand for more digital security in the virtual world. Cyber Crime is difficult to fight against and therefore intelligent cyber democratic concepts and solutions for open security questions and security leaks must be found with priority. Having these security-related concepts and solutions implemented appears to be an important prerequisite for the successful establishment of a Cyber Democracy. This must, however, also be seen in the area of conflict between freedom versus security: Any gained new degree of digital security may at the same time be perceived as a restriction of freedom. Especially the question how democratic processes can be protected against manipulation or increasing supervision by influential interests is of essential importance in the context. The anonymity of the Internet should also not be underestimated, as it appears to be a very valid question, whether the people actively participating in a Cyber Democracy using a web identification would be exactly the same persons in the real world.

Cyber Attacks Are the New Form of War Against Democracy in a Cyber Democracy

Digital attacks against democracies will be the wars of the future. Especially terrorists will be able to perform targeted attacks against selected nations. On the contrary to former times, where an army was needed to damage a state, only a few highly qualified computer programmers will be needed today. As one counter measure the computer networks of a democracy must be separated, better protected, and newly developed. In order to protect the democratic system and its citizens in the virtual world, a Cyber Democracy therefore requires qualified personnel. Currently many states are extremely poor protected against these cyber threats. As supervision and control can as well be automatically performed a Cyber Democracy can run into severe problems because of intelligent computers or highly sophisticated computer systems operated by the attackers.

Cyber Democracy Needs Appropriate Frame Conditions

It is extremely important that politics are creating appropriate frame conditions supporting the increasing usage of the Internet as well as the development of the institutions, techniques, and tools needed for a functioning and future proof Cyber Democracy. Initiatives must be started with highest priority for connecting Europe and the other continents of the world and its people all over the countries to the Internet and for ensuring safe and protected connections to the communication networks. In this context, the question of the citizen's access to the Internet and the communication networks must necessarily be clarified centrally and universally.

Cyber Democracy Means Interconnectedness of Politics with the Civil Society
The presidential election in the USA during the year 2008 has shown that a very well-connected candidate and a candidate presenting himself as a friend of the common people can win elections. The connectivity of politics and the leading candidates with the civil society will in future play an increasing role in a Cyber Democracy but as well during an election campaign in a classical democratic system. The ones using the modern media in the best way will therefore have the best chances to win democratic elections. Even if these first observations can be made, the change to and the impact of higher interconnectedness must be reflected better and more profoundly researched by the political sciences when describing the reference models for a functioning Cyber Democracy.

Cyber Democracy Means Loss of Freedom and Privacy
When talking about Cyber Democracy, it must also be stated that it is very difficult to delete data collected and stored in the virtual world of the Internet. Everything done by people in the virtual world of the Internet will be kept stored in some form. Through the Internet, people have already gained and will continue to gain new possibilities and global communication became a lot easier, but the digital human being is fully transparent and must be aware about his loss of freedom and privacy.

However, in 2016 a Cyber Democracy can be a very useful additional tool to share political information and knowledge with the population. This knowledge and information system in the form of a Cyber Democracy should according to our opinion not serve as the basis for the selection of political parties or the conducting of public opinion polls, but as a valuable tool for the civic education. Diecker and Galan explain "a clear precondition would be a cyber-public sphere capable of allowing for stronger involvement of citizens in democratic procedures." (Diecker and Galan 2014, p. 239) In the digital era facing increasing information overload, this will help the people to find orientation in the political environment, to support the formation of opinions, and to allow and support the political education. However, there is a need to develop a concept of Cyber Democracy for the future.

Conclusion

Based on better and better technical standards, the concept of a Cyber Democracy appears to be plausible and sustainable. Based on the underlying democracy theory and the concepts of measuring democracy quality, the existing characteristics of quality of democratic societies were shown. It appears, however, visible from the discussion about Cyber Democracy that a going towards a Cyber Democracy has implications, which could deeply endanger an existing democracy as well as its underlying democratic elements.

When connecting the results of the global analyses of the quality of democracy with the potential implications of a Cyber Democracy, we can confirm our thesis that a Cyber Democracy should only be implemented and sustainably maintained together with fulfilling important prerequisites. These prerequisites are the full

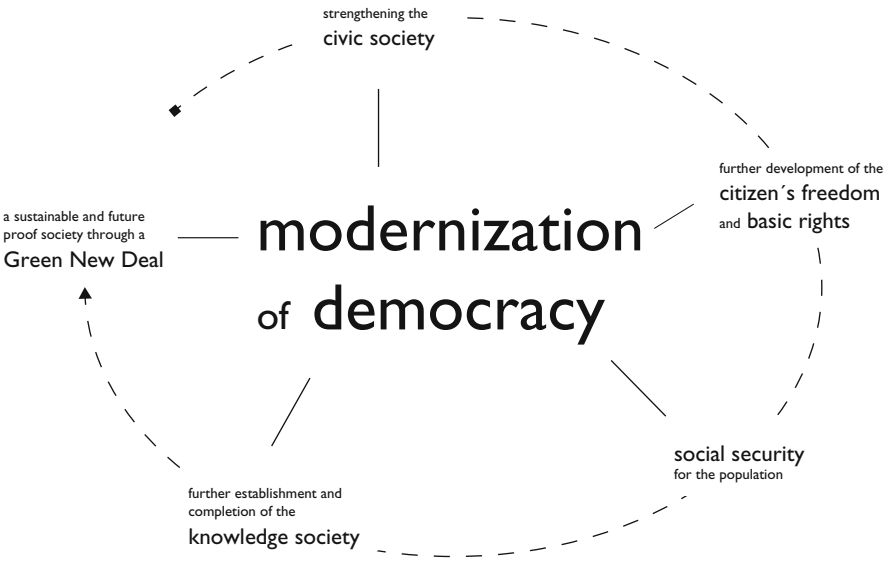


Fig. 5 Modernization of democracy (Source: Barth/Schlegelmilch 2014, p. 205)

compliance with the basic principles of a democracy as well as the quality standards for a high-quality democracy in an extremely high degree. Democracies only meeting the quality standards for a *medium*- or *low-quality* democracy do currently not meet the basic prerequisites for ensuring and safeguarding democracy in the real as well as in the virtual world.

Our statement therefore is that the risks resulting from a Cyber Democracy are predominant and as well not sufficiently controllable, as there can even with state of the art technology be no full protection against risks in the virtual world. A rethinking about the classical form of a democracy is needed and the concepts for a Cyber Democracy must be reworked. Generally it is correct and advisable to think about new forms and the modernization of democratic systems (see, e.g., Carayannis et al. 2012). This apparent need for thinking about modernization is however also needed for the current democratic societies and can be summarized with the following five points (see Fig. 5):

1. Strengthening the civic society through increased representative participation, e.g., with using more classical referendums for political decisions (= more direct democracy in the classical democracies)
2. Further development of the citizen's freedom and basic rights
3. More social security for the population, e.g., with ensuring a livelong basic income
4. Further establishment and completion of the knowledge society
5. The building up of a sustainable and future proof society through a Green New Deal on national and supranational level and in subsequent steps also on global scale

Democracies representing a high degree of democracy quality in the real world and having in place instruments for democratic modernization in a steadily changing world therefore do have the best prerequisites for creating a basic and sustainable concept of a Cyber Democracy in the digital world.

As a summary after evaluating the quality of democracy in the world 2015 and the chances and risks of a Cyber Democracy, it becomes clear that at this point in time in the year 2016 the model of the Cyber Democracy is bearing a too high risk for the idea of the democracy. The democracy in the form of a Cyber Democracy should even with current best available technology only be seen as a useful additional tool for the transmitting, sharing, and collecting of information. A Cyber Democracy supporting and executing direct democratic decisions and operating direct democratic processes can at this point in time not be recommended. The main reason for this is that any activity performed virtually in the course of participating in the democratic processes and with potentially big impact on the citizen's lives is in danger of being attacked, supervised, or decisively manipulated by enemies, terrorists, or other interested parties. Recent cases of Cyber Attacks and actual examples of digital wiretap operations as well as surveillance attacks against the population are supporting these arguments. From our perspective, a Cyber Democracy is currently not able to fulfill the two minimum democratic guidelines and standards for decision making in a democracy of being "free" and being "secret." Mainly this difficulty can have a far reaching impact on the political system of the democracy, undermine the common welfare and on the long run damage the quality of live in a democracy, which is based on and coming from freedom and equality.

References

Barth, T. D. (2010). *Konzeption, Messung und Rating der Demokratiequalität. Brasilien, Südafrika, Australien und die Russische Föderation 1997-2006*. Saarbrücken: VDM-Verlag Dr. Müller.

Barth, T. D. (2011). The idea of a green new deal in a quintuple helix model of knowledge, know-how and innovation. *International Journal of Social Ecology and Sustainable Development (IJSESD)*, *2*(1). http://www.igi-global.com/article/idea-green-new-deal-quintuple/51633

Barth, T. D. (2013). Freedom, equality and the quality of democracy: Democratic life in the United States, Australia, Sweden and Germany. *International Journal of Social Ecology and Sustainable Development (IJSESD)*, *4*(1). http://www.igi-global.com/article/freedom-equality-quality-democracy/77345

Barth, T. D., & Schlegelmilch, W. (2014). Chapter 7. Cyber democracy: The future of democracy?. In E. G. Carayannis, D. F.J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense* (pp. 195–206). New York: Springer. http://link.springer.com/chapter/10.1007/978-1-4939-1028-1_7

Bühlmann, M., Merkel, W., Müller, L., & Weßels, B. (2008a). Wie lässt sich Demokratiequalität am besten messen? Zum Forumsbeitrag von Thomas Müller und Susanne Pickel. *Politische Vierteljahresschrift, 49*(1), 114–122.

Bühlmann, M., Merkel, W., Weßels, B., & Müller, L. (2008b). *The quality of democracy: Democracy barometer for established democracies* (pp. 1–64). Working paper no. 10a – NCCR democracy. Retrieved from, http://www.nccr-democracy.uzh.ch/publications/workingpaper/pdf/WP10a.pdf

Campbell, D. F. J. (2008). *The basic concept for the democracy ranking of the quality of democracy*. Vienna: Democracy Ranking. Retrieved from, http://www.democracyranking.org/downloads/basic_concept_democracy_ranking_2008_A4.pdf

Campbell, D. F. J. (2014). Cyber-democracy. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense* (pp. 113–116). New York: Springer. Part II.

Campbell, D. F. J., & Barth, T. D. (2009). Wie können Demokratie und Demokratiequalität gemessen werden? Modelle, Demokratie-Indices und Länderbeispiele im globalen Vergleich. *SWS-Rundschau, 49*(2), 209–233. http://www.uni-klu.ac.at/wiho/downloads/campbell_u._barth-demokratiemessung-sws_rundschau-heft_2009_02-FINAL.pdf

Campbell, D. F. J., Pölzlbauer, P., Barth, T. D., & Pölzlbauer, G. (2012). Democracy ranking 2012: The quality of democracy in the World: Method and ranking outcome. Comprehensive scores and scores for the dimensions. Vienna: Democracy Ranking. http://democracyranking.org/wordpress/?page_id=392

Campbell, D. F. J., Barth, T. D., Pölzlbauer, P., & Pölzlbauer, G. (2014). *Democracy ranking – edition 2014: The quality of democracy in the World*. Norderstedt: Cambridge Scholars Publishing.

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "quadruple helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46* (3/4), 201–234.

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69.

Carayannis, E. G., Barth, T. D., Campbell, D. F. J. (2012). The quintuple helix innovation model: Global warming as a challenge and driver for innovation. *Journal of Innovation and Entrepreneurship*, *1*(1), 1–12. http://www.innovation-entrepreneurship.com/content/pdf/2192-5372-1-2.pdf

Dahl, R. A. (1971). *Polyarchy, participation and opposition*. New Haven/London: Yale University Press.

Diamond, L., & Morlino, L. (2005). Introduction. In D. Larry & L. Morlino (Eds.), *Assessing the Quality of Democracy* (pp. ix–xliii). Baltimore: The John Hopkins University Press.

Diecker, J., & Galan, M. (2014). Chapter 9. "Creating" a public sphere in cyberspace: The case of the EU. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense* (pp. 231–255). New York: Springer.

Ferdinand, P. (2003). Chapter 21. Cyber-democracy. In R. Axtmann (Ed.), *Understanding democratic politics: An introduction*. Sage: London. Online Pub. Date: May 31, 2012 , https://doi.org/10.4135/9781446220962, Print ISBN: 9780761971832, Online ISBN: 9781446220962.

Fröschl, E., Kozeluh, U., & Schaller, C. (Eds.). (2008). *Democratisation and de-democratisation in Europe? Austria, Britain, Italy, and the Czech Republic – A comparison*. Innsbruck/Vienna/Bozen: Studien.

Klein, A., Vöhringer, B., & Krcmar, H. (1999). Cyberdemocracy – eine politische chance. http://www.winfobase.de/lehrstuhl/publikat.nsf/intern01/076790EF7CDE06A84125686C002CCFCD/$FILE/99-19.pdf

Lincoln, A., Chittenden, L. E. (2009/1908). *Abraham Lincoln's speeches, general books*, Cambridge Scholars Publishing.

Lincoln (1863). Gettysburg Address; In Lincoln, A., Chittenden, L. E. (2009/1908). *Abraham Lincoln's speeches, general books*, Cambridge Scholars Publishing.

Lipset, S. M. (1960). *Political man* (1st ed.). New York: Doubleday & Company, Inc..

Macpherson, C. B. (1973). *Democratic theory. Essays in retrieval*. Oxford: Clarendon Press.

Mitterlehner, B. (2014). Chapter 8. Cyber-democracy and cybercrime: Two sides of the same coin. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense* (pp. 207–230). New York: Springer.

NCCR (National Center of Competence in Research). (2011). Democracy barometer – Newsletter. No. 8 February 2011. Retrieved from, http://www.nccr-democracy.uzh.ch/research/module5/barometer/Newsletter_Febr11_Demokratiebarometer.pdf

O'Donnell, G. (2004). Human development, human rights, and democracy. In G. O'Donnell, J. V. Cullell, & O. M. Iazzetta (Eds.), *The quality of democracy. Theory and applications* (pp. 9–92). Notre Dame: University of Notre Dame Press.

O'Donnell, G. (2005). Why the rule of law matters. In L. Diamond & L. Morlino (Eds.), *Assessing the quality of democracy* (pp. 3–17). Baltimore: The John Hopkins University Press.

Pelinka, A. (2008). Democratisation and de-democratisation in Austria. In E. Fröschl, U. Kozeluh, & C. Schaller (Eds.), *Democratisation and de-democratisation in Europe? Austria, Britain, Italy, and the Czech Republic – A comparision* (pp. 21–36). Innsbruck/Wien/Bozen: Studien.

Rueschemeyer, D., Stephens, E. H., & Stephens, J. D. (1992). *Capitalist development & democracy*. Chicago: University of Chicago Press.

Taureck, B. H. F. (2010). *Gleichheit für Fortgeschrittene – Jenseits von "Gier" und "Neid"*. Munich: Wilhelm Fink.

Thorsten D. Barth is employed at the Austrian Government. He studied political sciences and graduated with a dissertation (Dr. phil.) at the University of Vienna (Austria) and is a graphic designer. His research interests are research, technology, and the quality of democracy.

Willi J. K. Schlegelmilch is employed as a manager in the automotive industry. He holds responsibility for designing and implementing purchasing, invoicing, and accounting processes and systems for a worldwide sales organization. His research interests are the quality of democracy, information management, and system design.

Media in Knowledge Democracy and Cyber-Democracy

20

Wieland Schneider and David F. J. Campbell

Contents

W. Schneider (✉)
Die Presse, Vienna, Austria
e-mail: wieland.schneider@diepresse.com

D. F. J. Campbell
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@uni-ak.ac.at; david.campbell@aau.at; david.campbell@univie.ac.at; david.campbell@donau-uni.ac.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_12

Abstract

Media, particularly in combination with the Internet and advanced IT (information technology), can produce a major impact on politics. Elections, campaigning, governance, and policy-making in advanced democracies, but also in emerging democracies, do of course refer to media. It is also being said, and at least being discussed, that or if the media and new media were playing a triggering role for the events of the Arab Spring. New media and the New Social Media are also acting that invasive, because they can easily operate beyond and transcend national borders, and they allow the "cost-efficient" bypassing of more traditional media forms that are very cost intensive. This poses dangers for democracy. But this also poses opportunities for democracy and knowledge democracy, in the sense of offering a broader spectrum of available and accessible information. In addition, the analysis here also emphasizes and refers to this interesting interdisciplinary, transdisciplinary, and inter-sectoral overlap of media, knowledge democracy, and innovation systems. Media, new media, and New Social Media impact politics, but they may also enhance innovation and innovation system. The theories and concepts of the Quadruple and Quintuple Helix innovation systems are explicit about the role of media for knowledge and innovation ("media-based and culture-based public"). Media allow and support the integration of knowledge creation, knowledge production, and knowledge application across diverse national, regional, and global innovation systems. In that sense, media may also be an element and a force for the advancement of AI (artificial intelligence) and AI systems. Already existing examples here are robot journalism, robot writers, and robot writing. The media are interlinking and building networks between political processes in media democracy and innovation processes in innovation systems. Between the sectors of the political system and of the innovation systems, new forms of cross-connectedness are emerging, facilitated also by the media.

Keywords

Artificial intelligence (AI) · Cyber-democracy · Innovation · Knowledge democracy · Media · New media · New Social Media · Robot journalism · Robot writer · Robot writing

Introduction

In this analysis, we want to explore (further) how media and new media (also New Social Media) are relating to knowledge democracy and cyber-democracy. Cyber-democracy is being understood as an advanced form or manifestation of knowledge democracy, where of course also mature IT (information technology) is playing a lead role in it. Our analysis is explorative in character, meaning that we refer to innovative concepts and innovative political examples, but do not assert to have developed already

a comprehensive picture. The status of our analysis is preliminary, and the first findings or assertions of our analysis should be understood as propositions or hypotheses.

When there is a saying about *media and new media and New Social Media*, so what exactly is here the difference (or what is the overlapping)? In this distinction, the "media" sometimes are also being paraphrased as the "traditional media," for example, print, television, or radio. *New media and New Social Media will often have a connection to the Internet and to electronic (and virtual) forms*. This may mean that the access to electronic, Internet-based media and media content is free (free of cost), implying that the content can diffuse globally at fast rates. Also the production of electronic, Internet-based media and media content can be (almost) for free. So here, the new media apply and employ also new economic principles, referring to knowledge economy. At the same time, this also has references to knowledge democracy in terms of cyber-democracy. However, it also must be emphasized that not all forms of production of and access to new electronic, Internet-based media is free of costs: some models imply even the involvement of substantial (financial) resources. Furthermore, there exist also several variations of hybrid co-development of forms of traditional media and new media and New Social Media. Basically, all (almost all) manifestations of print media and audio-visual media also will have in parallel a type of existence electronically on the Internet. Clear-cut distinctions, because of this, are more and more difficult, being challenged by modes of a continuous transition.

Our analysis is structured into four main sections. Section "Interdisciplinary, Transdisciplinary and Trans-sectoral Concepts of Media and New Media: Quadruple and Quintuple Helix Innovation Systems and Knowledge Democracy" focuses on conceptual models that link and interlink innovation with media. Here, the approach of *Quadruple and Quintuple Helix innovation systems* is offering a whole set of possible and integrative explanations. In section "Innovations and Innovative Developments in the Media," a broad overview of current and innovative developments in media is being introduced. Section "Case Studies on Media in Knowledge Democracy and Cyber-Democracy" presents in a detailed format two further case studies: one is referring to political developments and media developments in recent political presidential elections, and the other refers to the use of media by radical political Islam. In the conclusion (section "Conclusion"), a short outlook is being provided.

Interdisciplinary, Transdisciplinary, and Trans-sectoral Concepts of Media and New Media: Quadruple and Quintuple Helix Innovation Systems and Knowledge Democracy

Of the currently existing and evolving concepts and theories on innovation and knowledge democracy (cyber-democracy), there is already, in some cases and instances, an explicit reference of thinking about media, new media, and New Social Media. This is being achieved and furthermore emphasized very directly by the

so-called *Quadruple and Quintuple Helix Innovation* theory and systems (Carayannis and Campbell 2009, 2010, 2014). They build upon and extend the original model of Triple Helix that refers to university-industry-government relations (Etzkowitz and Leydesdorff 2000). In the Quadruple Helix, as fourth helix, society and democracy and, in the Quintuple Helix, as fifth helix, social ecology and the environment are being introduced and added, and they are being indicated as being crucial for knowledge production (research) and knowledge application (innovation). In more particular, the Quadruple Helix also speaks about the "media-based and culture-based public." Media play a crucial role in society and democracy and of course also for politics and the political system. There are notions such as "media democracy" or of the functioning of media as an additional "informal" or "fourth" branch of government (see, e.g., Hemer and Tufte 2005). However, media and Internet-based media also should be regarded as pivotal and crucial for the support and enhancement of innovation and innovation systems. In full, the Quadruple Helix adds as a fourth helix the elements of "media-based and culture-based public," the "civil society," and "arts, artistic research and arts-based innovation" (Carayannis and Campbell 2009, 2012, p. 14; Carayannis and Pirzadeh 2014; Campbell and Carayannis 2016; see also: Bast et al. 2015; Danilda et al. 2009; Eigelsreiter 2017; Hemlin et al. 2004; Mitterlehner 2014). *The Quadruple Helix, therefore, also could and should be emphasized as the perspective that specifically and particularly brings in the "dimension of democracy" or the "context of democracy" for knowledge, knowledge production, and innovation*. The Quintuple Helix innovation model already is more comprehensive, again in its analytical and explanatory stretch and approach, by adding also as the fifth helix (and perspective) the "natural environments of society" (Carayannis and Campbell 2010, p. 62; see furthermore Carayannis et al. 2012) (see Figs. 1 and 2).

Roeland J. in't Veld (2010a, b) developed an advanced and mature concept, how to frame further the structures and dynamics of and within a knowledge democracy. He places a particular emphasis on the role and responsibility of the media. For him, there are and operate three crucial forces as crucial references: "emerging participatory democracy," "emerging transdisciplinary design/science," and "emerging bottom-up media" (Veld 2010b, p. 11). The bottom-up media are complementing the more "top-down media." On the relationship of media and politics, Veld (2010b, p. 4) provides the following assessment: "Media and politics, a relationship based on mutual interest as on the other hand the media equally need politicians in order to produce news, one of their main products. So this dependence is reciprocal."

This multifold meaning and importance of media (and of new media and New Social Media) for (1) politics and the media democracy, on the one hand, and for (2) knowledge production (research) and innovation (knowledge application), on the other, underscores here (3) also interdisciplinary and transdisciplinary, even transsectoral, elements and characteristics of media and of their media functioning. By this, the media are interlinking and building networks between political processes in media democracy and innovation processes in innovation systems. *Between the sectors of the political system and of the innovation systems, new forms of cross-connectedness are emerging, facilitated by media*. Traditionally, analysis had

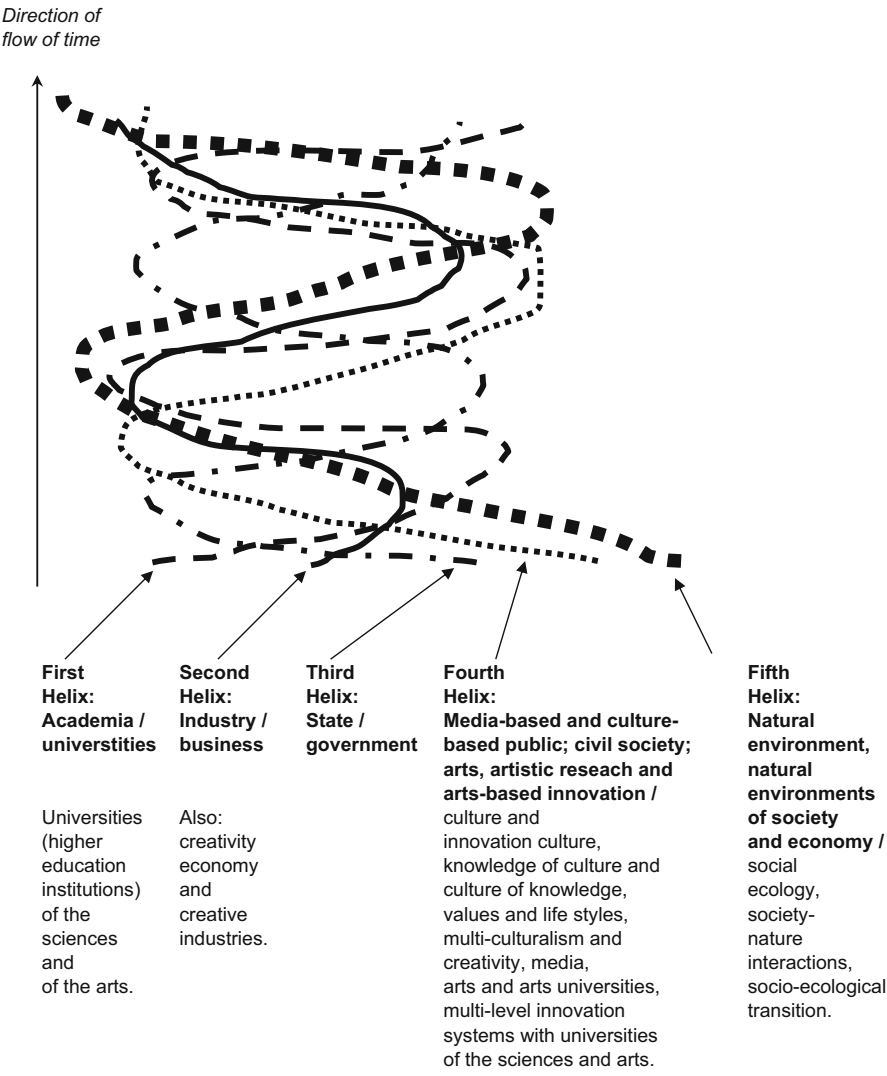


Fig. 1 The Quadruple and Quintuple Helix innovation systems. (Source: Carayannis and Campbell 2014, p. 15, Adapted from Carayannis and Campbell 2009, p. 207)

referred the media closer to the political and the political system. Now, possible functionalities of the media are being seen in a broader context of opportunities, again in the context of knowledge democracy and cyber-democracy.

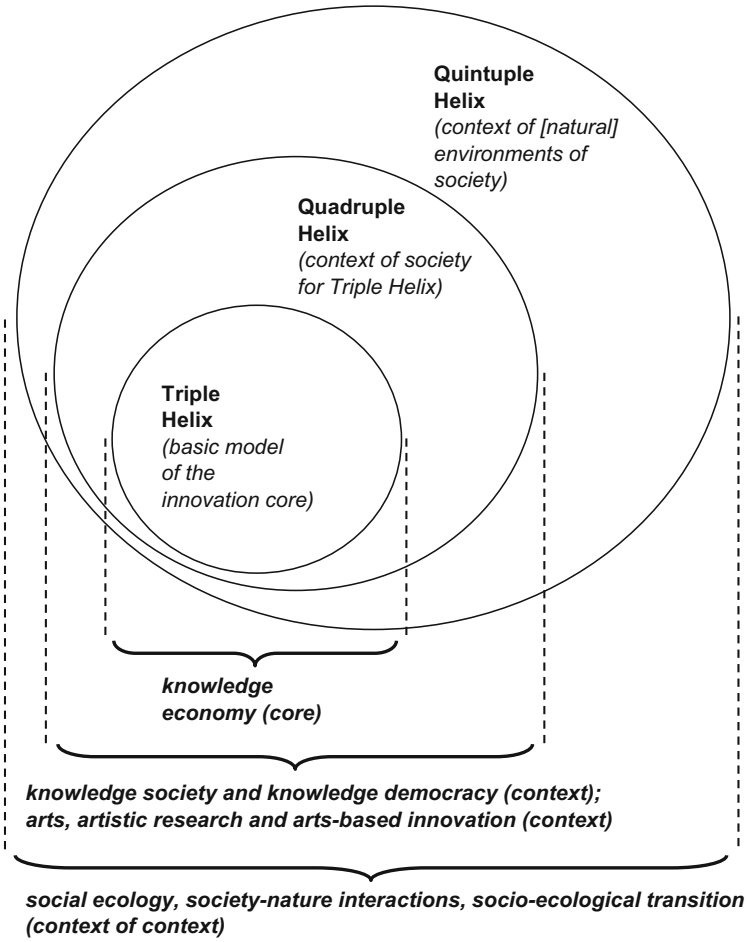


Fig. 2 The Quadruple and Quintuple Helix innovation systems in relation to society, economy, democracy, and social ecology. (Source: Carayannis and Campbell 2014, p. 6, Adapted from Carayannis and Campbell 2012, p. 4)

Innovations and Innovative Developments in the Media

The most important of all of the media-innovations are the online media with the different implications for communication. The Internet provides a new form of distribution of information, which is more "democratic," when being compared to the times when TV, print media, and radio ruled. Variations of citizen journalism have appeared, for example, new projects done and enabled by crowdfunding. In theory, a small crowdfunded group of journalists has a similar opportunity to get their messages out into the world, as easily as it is for the big mainstream media

trusts (media houses). The platform for this is the *World Wide Web* (WWW). This means that so-called mainstream media have to deal with a new type of competitor. Furthermore, it is also the competition for being recognized by the audience as a trustworthy source: Are these the so-called mainstream media or the small websites run by citizen journalists?

The Internet, also with social media tools such as Facebook and Twitter, has also a political function. There was a joke in Egypt after the fall of the authoritarian president Hosni Mubarak, back in February 2011: Mubarak meets the former Egyptian presidents Gamal Abdel Nasser and Anwar as-Sadat in the Hereafter. He asks Nasser: "How did you die?" And Nasser says: "By poison" – confirming old rumors in Egypt that Nasser did not die because of a heart attack but was actually murdered. Then Mubarak asks Sadat: "How have you been killed by your enemies?" And Sadat, who has been shot by assassins, says: "By a bullet." After a while, Nasser and Sadat ask Mubarak: "And what is about you? What has killed you?" And Mubarak responds: "the Internet."

Of course, it was not just the Internet alone that ousted Mubarak from political power. In the joke, Mubarak also could have mentioned (and cited) the increasing number of Egyptians, who were furious about his corrupt, "kleptocratic" regime, or the generals one step behind him, who just waited to take over power. But the Internet and social media were an important weapon for the opposition groups, who were responsible for the uprising on Cairo's Tahrir Square. The Internet and social media were a tool of information and communication and for coordination between the protesters in Egypt and also in other parts of the Arab world. "Friends from Tunisia explained to us on Facebook, what to do against teargas. And we passed this information on to our friends in Yemen," said, for example, Sayed Elsisi, a young man, who took part in the uprising on Tahrir Square (Schneider 2012, p. 18). After the 28-year-old Egyptian Khaled Said was killed by police officers in Alexandria, activists founded the Facebook page "Kullena Khaled Said" (We all are Khaled Said). The Facebook page went viral among young Egyptians and represented an important platform for the protesters on Tahrir Square. One of the masterminds behind this Internet platform was the blogger and employee of Google, Wael Ghonim (see: 2012). In order to silence the critical voices and to stop the flow of information between the protesters during the uprisings in January and February 2011, the Egyptian authorities shut down the whole Internet system and the mobile phone services in Cairo and in most parts of the country. But after some days, they had to open the Internet again. On the 4th of February 2011, the Organization for Economic Cooperation and Development (OECD) already had estimated that the shutdown of the Internet and communication services led to direct costs of at least 90 Million US dollars, not including secondary economic impacts from losses of business in other sectors such as tourism or call centers (http://www.oecd.org/sti/ieconomy/theeconomicimpactofshuttingdowninternetandmobilephoneservicesinegypt.htm). A contemporary economy and economic system cannot afford to exist without a functioning Internet system. This shows how difficult it is, even for an authoritarian regime, to control the subversive tool of the Internet.

The new forms of social media on the Internet indicate also new sources of information for so-called mainstream media. In the past, news agencies, such as

Reuters, Associated Press (AP), Agence France-Presse (AFP), Deutsche Presse-Agentur (DPA) in Germany, and the Austria Presse Agentur (APA), all played an important role for distributing breaking news to journalists, especially to the "foreign desks" of the different media houses. They still do so. But nowadays, there is also a new type of news agency: it is Twitter. It is a very fast way of putting out news, and in most of the times, it is faster than the official news agencies. In war zones such as Syria, it represents sometimes the only link to the outside world. You have, for example, small opposition groups operating from areas controlled by the so-called Islamic State and against the "Islamic State" (different acronyms being used for the Islamic State are IS/ISIS/ISIL/DAESH). These resistance groups spread the information about their situation via Twitter or Facebook. There is, for example, "Raqqa is Being Slaughtered Silently" (@Raqqa_SL and http://www.raqqa-sl.com/en from the ISIS-"capital" Raqqa in Syria) or "Mosul Eye" (@MosulEye from the Iraqi city of Mosul). An important source for international media, reporting about events in Syria, is the "Syrian Observatory of Human Rights" (SOHR), @syriahr, which is based in London. SOHR represents an NGO, collecting reports from Syria and distributing them via social media tools, for example, Twitter. SOHR stands in opposition against the Syrian regime and against Jihadi groups, e.g., ISIS (ISIL). At the same time, SOHR is being considered to provide accurate and reliable information.

In some of the cases, it is clear and being openly said that Twitter accounts are the official accounts of organizations, parties, and identifiable actors: for example, the account of the so-called People's Defense Units (YPG); the armed forces of the mainly Kurdish-inhabited cantons in northern Syria, Rojava Defense Units @DefenseUnits; the official account of the regime of the Syrian president @Presidency_Sy; the rebels of the "Free Syrian Armee" (FSA) @FreeSyrianArmy; or the so-called Islamic Front @islamic_front or @IslamicFront_En – the biggest umbrella organization of the Anti-Assad-rebel-forces.

In other cases, however, it is not so obvious, for example, if it is an account of a citizen journalist, reporting from one of the hotspots of the Syrian war, Aleppo. The citizen journalist represents no official organization, but she or he might be a political activist and has a particular political agenda. Or they might be under pressure of the groups that are controlling the region. Or they might even try to be independent. But to live in a city that is being bombed, and to be at the same time "politically neutral," this is difficult to achieve. However, in some cases these citizen journalists are the only available source of information from surrounded cities exactly like this was the situation in Aleppo.

This again refers to a question that has always been a key question for journalists: What is a reliable source? Thanks to the Internet and social media, the number of potential sources has grown. Opposition groups in authoritarian countries or people in war zones receive and are being granted the possibility to spread their voices directly to the world. And journalists, observing this flow of messages from the outside, can report about this and make these voices even stronger with an amplifying effect. At the same time, however, this development makes it also easier to spread propaganda through social media. The dangers are growing that journalists take over this propaganda and furthermore pass it on to their audiences. In the past, there was more time for a journalist to check and to control information. With

Internet and online journalism, the time frame for checking information is shrinking considerably. When a journalist is working for online media, the pressures there are to publish the breaking news immediately. If the information is coming from a reliable professional new agency, there is clearly less of a danger that the information is not accurate. But if the information is coming directly from a Twitter source, then the risk is higher that the information may not be accurate.

News agencies are being mainly used by professional media, companies, or the staff of politicians, who have to pay to access these information services. But information, spread by social media such as Twitter, is open to and for everybody. This means: if somebody is publishing "breaking news" on Twitter, then the information (or rumor) is out. And traditional media must react quickly, because their audiences already have been exposed to the social media. Should professional media need too much time for checking information (before redistributing, verifying, or denying it), the already informed audience might become impatient and may think that "mainstream media" are trying to "hide" something. Or that traditional media are useless for a fast and rapid information access. The resulting question for the consumer therefore is: Do I still need professional media to receive information?

On the other hand, Twitter, Facebook, and other forms of social media are also being used by news agencies, newspapers, and other organizations of professional media, to spread their messages and stories. Online platforms indicate new opportunities for media companies. They can attract direct feedback from their online readers. Journalists see immediately, which articles are generating the most clicks, which stories are working (the best), and which are not. This creates and opens a new way to meet the demands (sophisticated demands) of the audience. More clicks lead to more economic success for media house. But this trend also has a problematic impact. One of the difficult tasks of professional journalism is the selection of news: What is more important in order to understand political or economic developments, what is less important? Receiving a direct feedback by clicks might be a temptation for journalists to rely too much on this feedback, when selecting stories. Then journalists would switch over to become "salesmen of infotainment" and would lose their role of "gatekeepers for important news."

Online media also introduce new opportunities of direct communication between journalists and their audience. Consumers of online stories have the possibility to comment on articles through postings. Journalists, on the other hand, have the possibility to find out, what the audience is thinking about the different topics. This is quite important for a more democratic discussion between journalists and the (their) audience. But there lies also a danger in it: media companies might try to sell to their consumers what the consumers want to read or hear. Furthermore, political or other interest groups may use the tool of postings to lead the online discussion (and even the reporting of the journalists) into a special (and particular) direction.

This new environment brings also new challenges for the work of journalists. As already mentioned, in online journalism there is less time to check information. Because of the variety of new media platforms, journalists have to work in a broader variety of fields and contexts. In several of these cases, "multimedia" in professional media means that everybody should do everything herself or himself: from print

articles to online articles and short videos for online. This is because in most of the media houses, there is not enough money to employ specialists for these different ways (and tasks) of storytelling. On the other hand, there are new tools, which should make journalism quicker and furthermore more cost-effective. One of these tools is the so-called robot journalism (robot writer). The computer is able to write (self-write) a story independently through an algorithm (http://www.nytimes.com/2015/03/08/opinion/sunday/if-an-algorithm-wrote-this-how-would-you-even-know.html?_r=0). The LA Times, for example, is already working with this technology. After an earthquake in the March of 2014, they published an article about this online within 3 min, faster than their competitors (http://www.bbc.com/news/technology-26614051). This type of technology is also being used for business stories and sports reporting, for example, by Associated Press (AP):

http://www.bbc.com/news/technology-34204052
http://www.rdmag.com/news/2016/01/fourth-industrial-revolution-and-robot-journalism
http://www.techtimes.com/articles/93473/20151010/ap-has-a-robot-journalist-that-writes-a-thousand-articles-per-month.htm

Online audiences are in a position of consuming *information a la carte*. They can get and access what they want to read, hear, or see from different platforms. The positive impact is that it is easier today, to receive a broad and broader view of information and opinions. For this the audience may utilize a variety of different sources. The problematic impact is that consumers are able to just pick out those analyses, commentaries, and opinions that they want to have and want to deal with. But then they stay and remain within their own ideological information ghettos.

Such algorithms also could produce stories, which fit exactly the different consumers. The computer knows where users are living, what they are looking for in Google, and so on. This brings several advantages for media houses in meeting the progressing consumer demands. But these specifically tailored news, information, and infotainment elements feed also the problems already mentioned, namely, in reproducing particular and fragmented niches within the whole information spectrum. But algorithms, robot writing, and robot journalism clearly express how AI (artificial intelligence) already is meeting the world of media.

Case Studies on Media in Knowledge Democracy and Cyber-Democracy

Example One: Media and the Phenomenon of Elections in Western Democracies

In the years 2016 and 2017, there were several political presidential elections, which had caused international attentions. These were the elections in Austria, France, and the USA (United States), where the presidential outcome was determined by a direct

popular vote and where the final political outcome made a difference. Partially the voting trends did differ in these three countries, but partially they also had in common several comparable trends (Campbell et al. 2015; CNN Politics 2016; Financial Times 2017; Helms 2012a, b; Spiegel Online 2016; The Telegraph 2017a, b; Wineroither and Kitschelt 2012; Xavier and Campbell 2014; Zandonella and Perlot 2016a, b). *When the focus is now on the question, which political trends and which political innovations became manifest in these three elections, then also the media, and more particularly the new (Internet-based) media, became manifest in playing a role, which may even increase in the future (the political future of democracy)*. In the following, we want to introduce a few propositions for further discussion (see also Campbell et al. 2017):

1. **The New Right focuses on the working class, and the New Left focuses on the middle class (Proposition #1)**: In western democracy, a conventional voting behavior pattern has been that the (lower) working class was in support of the political left and the (higher) middle class in support of liberal of conservative forces (the "political right"). There is the assertion of a partial political alienation of the working class with the left. Reasons for this are fears that the working class cannot participate anymore in economic progress and that the inequalities and divisions increase. This the New Right (right-wing populist parties and politicians) sees as an opportunity for trying to attract the working class, often in association with national or nationalistic programs. This "to the right" leaning of the New Right, however, then can mobilize a counter-movement in the middle class that fears the radical agenda of a New Right. For the New Left (moderate, centrist, liberal, green, or ecological parties and politicians), this identifies an opportunity for attracting and drawing-in electoral support from the middle classes, also in an attempt to neutralize possible gains of the New Right in other segments of the population. Put in other words, there is a partial political alienation between the middle class and the New Right (Campbell 2016). In that sense, the voting rationale of Traditional Left against Traditional Right is contrary to New Left against New Right. However, the axis of competition between New Left and New Right has not replaced the axis of Traditional Left and Traditional Right; they both continue to coexist. This, obviously, complicates political markets and political competition.
2. **There has not been a general political swing to the right in the presidential elections of 2016 and 2017, perhaps even the contrary, an anti-rightist-swing, was the case (Proposition #2)**: The to-leave-majority in the UK Brexit referendum of June 2016 often was interpreted to represent a victory that associates closely with ideas with a right-wing populist character. When the focus is on the three identified presidential elections, however, the picture is quite contrary. In institutional terms, the more-to-the-right-leaning Donald Trump has won the US presidential elections. But based on the popular vote, not Trump, but the more-to-the-left-leaning Hillary Clinton actually won the race. Because of the specific institutional setup and design of the state-wise electoral colleges in the United States, the popular-vote-defeat of Trump was translated into an electoral-college-

victory of Trump. In a theoretical reasoning about democracy, there are probably good arguments that the popular vote should be regarded as being more important when being compared with any other institutional rearrangements of votes. In the context of presidential elections in France and Austria, there only the popular vote counts (particularly for the runoff phase), and every outcome contrary to popular-vote-majorities would be considered to represent a case of "electoral fraud." How has the institutional victory of Trump played into other presidential elections in Europe? There were speculations that this may benefit the political right in general. However, in the presidential runoff voting cycles in Austria and France, the candidate of the right (right-wing populist in Austria and far right in France) was always defeated by the left challenger (Austria) or centrist challenger (France). Therefore, in this particular framing, the institutional victory of the more-to-right-leaning Donald Trump in the United States has had in Europe perhaps even a contrary effect, producing a political swing to the left or at least an anti-right-swing and move against the political right in continental Europe. In that sense, the political swings in the United States were (are) contrary to political swings in other countries (with an advanced democracy). However, based on the popular-vote-results, the recent presidential voting swing in the United States (2016) was in fact similar in tendency when being compared with Austria and France.

3. **The partial shift from a party democracy to a politician democracy and the opening of political parties for political newcomers and political independents (Proposition #3)**: In a democracy (and advanced democracy), how important are political parties and how important are the individual politicians? There is the assertion of a gradual trend of an increase of the influence and importance of individual politicians, while the parties are suffering, at least partially, from a decrease in importance. Still, the political parties are important and do matter. But the individual politicians and the political party leadership may matter even more. Political diversity and heterogeneity can increase when new so-called third parties are entering the political field (and market). However, equally important is the move and push of political parties to open the parties for political newcomers and independents or to create alliances (voting alliances) and networks of the political parties with civil society. Back in the US presidential election of 1992, (more-to-the-right-leaning) Ross Perrot had run as an independent candidate, but had lost, even while attracting a 18.9% share of the popular vote. By many, Donald Trump was not being considered as a typical Republican. Trump did not have a professional track record in politics. But Trump did not decide to run as an independent, but to participate in the primaries of the Republican party, and by securing their nomination he could rely on the platform and networks of the Republican party in support of his candidacy for US presidency in 2016. Primaries (preelections) represent one approach for widening the boundaries of a political party. Another option for political parties is either to allow political newcomers or political independents to run on voting tickets of the party or to craft network-style voting alliances of political parties with civil society (representatives). This should increase the attractiveness of political parties to-be-voted and grants a greater importance to individual politicians. Thought about

consequently, the political (election) leaders of a political party would not have to be party members in a formal sense. In the French presidential elections of 2017, Emmanuel Macron was not the front-runner and candidate of any of the established political parties, but ran as an independent, but with support of the newly and flexibly organized party En Marche, which he had formed a year earlier back in 2016. With his presidential victory in May 2017, Macron reorganized En Marche to La République En Marche, which ran for the French national legislative elections in June 2017. La République En Marche comes close in resembling a centrist party. At the same time, the party was designed to represent a network alliance of a traditional political party with civil society, since a substantial share of positions on the electoral list of candidates was reserved for political newcomers and independents (without a longer professional political record in the past). Also, the list of candidates was balanced in terms of gender criteria with a female and male equality. In the French national legislative elections of June 2017, La République En Marche produced a huge victory and won an absolute majority of 308 seats (out of a total of 577 seats).

4. **The political media markets are changing, with a growing importance of New Social Media (new media) and the Internet, but also the dangers of cyberattacks are increasing (Proposition #4)**: Increasingly, distinctions are being drawn between the established traditional media and the so-called New Social Media. Sometimes, the established traditional media are being additionally classified as "Top-down Media" and the New Social Media as "Emerging Bottom-up Media" (Veld 2010a, b, pp. 9, 11). Both media forms are also rooted in the Internet, but for the New Social Media, the Internet is even more important. In fact, the New Social Media exist (more or less) only via the Internet. One key characteristic of New Social Media is that they can be produced, reproduced, and distributed through the Internet at almost no cost. Messages are being diffused and "go viral" with zero expenses. What can matter is the degree of name recognition, level of awareness, familiarity, and reputation of the New Social Media organization (or network of the message carrier). There are controversial debates, to which extent the demands for more democracy during the Arab Spring were sparked or amplified by New Social Media (Xavier and Campbell 2014). Different types of New Social Media and the different formats of the Internet have the potential to impact how political campaigns or political elections are being carried out (see, furthermore, Kaiser et al. 2017; Bernhardt and Liebhart 2017). Furthermore, there are partial asymmetries, which types of media are being addressed by which types of politicians or political parties. It is being said that particularly populist or right-wing populist politicians and political parties are inclined to utilize the New Social Media formats, because the established traditional media often view such populist political manifestations more critically. Also, politicians now have the chance to establish their own information and message channels through such New Social Media and by this become more independent from the established traditional media. For example, the US president Donald J. Trump has his own publicly accessible Facebook account, which was subscribed by almost 24 million persons as of July 2017. By March 2018,

this figure had increased to about 24.4 million persons (https://de-de.facebook.com/DonaldTrump/). This increasing Internet orientation of the media markets makes political communication and elections potentially vulnerable to cyber-attacks (from inside or the outside). It is being said that consequent (massive) cyberattacks took place in the United States during the presidential campaign of 2016. The primary source of cyberattacks should have been a foreign power. There is the assertion that the Russian government (may) have tried to intervene with various strategies into the US elections in a way so to harm particularly the prospects of the more-to-the-left-leaning Democratic candidate Hillary Clinton. On this subject the US Senate Select Committee on Intelligence (2017) also launched a systematic investigation.

Example Two: Media and the Phenomenon of ISIL (ISIS)

Radical anti-democratic political movements, which assert to be influenced by Islam, pose a serious problem. In theoretical terms, a "caliphate" represents a premodern (in that sense a pre-democratic) political concept for the political organization of a state, which does not apply principles of separation of power between the different branches of government in a democratic tradition but implies a combination and falling-together of political and religious leadership. Caliphates assert to stand in line of a direct legacy and continuation with the establishment and founding of Islam in the early seventh century. When the terror organization of ISIL, the "Islamic State of Iraq and the Levant" (sometimes also being translated as IS or ISIS, "Islamic State of Iraq and Syria"), issued the claim of having (re-)established a caliphate in 2014, in a certain sense, a political reality reemerged with connotations now 1400 years old. While other terrorist organizations, like Al-Qaeda, operate more in formats of an underground organization, ISIL is driven by the desire of forming and building state (quasi-state) structures, expressed in the understanding of having set up a caliphate. From an ISIL perspective, only military defeat would drive complete ISIL back into the status of an underground organization.

According to Wieland Schneider (2015), what makes ISIL so distinct and specific are (1) the levels of publicly demonstrated atrocities, (2) the introduction of slavery, but (3) also the way how ISIL managed these approaches in their media propaganda, using social media and videos. ISIL could and does tailor its media messages, depending on and differentiating between media markets, addressing Arab countries or Western societies in various and particular ways (Bösch 2017). For this, Schneider also introduces the term of "Jihadism" as a form of a "bizarre pop culture" (Schneider 2015, p. 213). All of this feeds into the interest of ISIL to build the quasi-state structures of a caliphate, supported and defended by ISIL insurgent groups in the West, so to strike there directly terrorist attacks. Furthermore, ISIL attempts to diffuse into other Arab countries, most notably Libya. In that sense, ISIL may also be interpreted as a fluid spectrum, ranging from underground groups on the one side, over to state building attempts on the other. These state-building efforts of ISIL make ISIL distinct (and to draw a line of difference against Al-Qaeda).

Early 2018, ISIL already had suffered from major (military) setbacks and was driven out of most of the territories in Iraq and Syria, meaning that ISIL had (has) to retreat to underground activities. So the ISIL-based caliphate had finally collapsed. What ISIL illustrates is that in the context of the Arab countries or of the Arab Spring, prodemocratic as well as anti-democratic political movements refer to the use (and employment) of new media and new-media-means. However, we want to arrive here at the vision that (in the long or longer run) democracy and further democratization will finally arrive in the Arab countries on a broader and more durable basis. No other outcome is acceptable or shall be accepted. This also aligns with beliefs that democracy and democratic development associate with sustainable development (Campbell and Carayannis 2014; Campbell et al. 2015). Cyber-democracy will have here its role and has all the potentials and capabilities to contribute and co-contribute to such a desired outcome (Xavier and Campbell 2017).

Conclusion

Media in knowledge democracy and cyber-democracy represent an area, where incremental but also radical innovations and innovative developments are taking place. There is advanced research, also interdisciplinary and transdisciplinary research, trying to capture and to explain these currently emerging phenomena (e.g., see Heikka and Carayannis 2016, 2017). *At the same time, however, a certain impression is manifest that on some incidences the research here is lagging behind the unfolding and evolving empirical phenomena in the "world of media" (the real worlds of media)*. Media, particularly in combination with the Internet and advanced IT (information technology), can produce a major impact on politics. Elections, campaigning, governance, and policy-making in advanced democracies, but also emerging democracies, do of course refer to media. Governance and policy-making are being marketed in the form of a continuous campaign approach (Filzmaier and Plasser 2001). It is also being said, or at least being discussed, whether or not the media and new media had an effect or were playing a triggering role for the events of the Arab Spring (Xavier and Campbell 2014, 2017).

New media and New Social Media are acting, pushing, and diffusing that invasively, because they can easily operate beyond and transcend national borders, and they allow the "cost-efficient" bypassing of more traditional media forms that are heavily cost intensive. This poses dangers for democracy (e.g., populist politicians regularly use New Social Media to bypass the traditional media and this for purposes of demagogy). But this also poses opportunities for democracy and knowledge democracy that have the potential to outweigh and to transcend the disadvantages. For example, progressive civil-society initiatives and organizations are in a position of utilizing New Social Media for supporting quality of democracy quite effectively.

In addition, our analysis also intends to emphasize and to refer to this interesting interdisciplinary, transdisciplinary, and inter-sectoral overlap of media, knowledge democracy, and innovation systems. Media, new media, and New Social Media

impact politics, but they may also enhance innovation and innovation system. The theories and concepts of the Quadruple and Quintuple Helix innovation systems are explicit about the role and importance of media for knowledge and innovation. Media also can facilitate the integration of knowledge creation, knowledge production, and knowledge application across diverse national, regional, and global innovation systems. In that sense, media act also favorable for the advancement of AI (artificial intelligence) and AI systems. Robot journalism, robot writers, and robot writing already serve as examples based on IT. Current or future forms of media and of new media (New Social Media) may require IT or other technological standards already rooted in AI, so to offer more complex services and a more complex functionality, *which again will feed back into processes of politics and processes of innovation*.

Cross-References

- ▶ Cyber-Democracy in the Middle East
- ▶ Libya: Where Cyber-Democracy Reached Its Limits – How the Case of Libya Challenges the Idea of Cyber-Development
- ▶ What Happened to the Public Sphere? The Networked Public Sphere and Public Opinion Formation

References

Bast, G., Carayannis, E. G., & Campbell, D. F. J. (Eds.). (2015). *Arts, research, innovation and society*. New York: Springer. http://www.springer.com/business+%26+management/technology+management/book/978-3-319-09908-8.

Bernhardt, P., & Liebhart, K. (2017). Politik auf Instagram: Bildstrategien von Norbert Hofer und Alexander Van der Bellen im Bundespräsidentschaftswahlkampf 2016. *SWS-Rundschau, 57*(2), 146–167.

Bösch, P. G. H. (2017). *Der "Islamische" Staat: Kalifat des Schreckens? [The "Islamic" State: Caliphate of Scare?]*. Vienna: Manuscript.

Campbell, D. F. J. (2016). *Wie Trump alle Prognosen über den Haufen warf. Nicht nur die Demokraten sind die Verlierer dieser US-Wahl, sondern vor allem auch die Meinungsforschungsindustrie (Guest Commentary)*. Vienna: Die Presse. http://diepresse.com/home/meinung/gastkommentar/5115547/Wie-Trump-alle-Prognosen-ueber-den-Haufen-warf?from=suche.intern.portal.

Campbell, D. F. J., & Carayannis, E. G. (2014). Explaining and comparing quality of democracy in quadruple helix structures: The quality of democracy in the United States and in Austria, challenges and opportunities for development. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 117–148). New York: Springer. http://link.springer.com/chapter/10.1007%2F978-1-4939-1028-1_4.

Campbell, D. F. J., & Carayannis, E. G. (2016). The academic firm: A new design and redesign proposition for entrepreneurship in innovation-driven knowledge economy. *Journal of Innovation and Entrepreneurship, 5*(12), 1–10. https://doi.org/10.1186/s13731-016-0040-1. http://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-016-0040-1.

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493. http://link.springer.com/article/10.1007/s13132-015-0246-7.

Campbell, D. F. J., Fabrykowska, A., & Drexler, A. (2017). Innovations in presidential elections: The United States, France and Austria in comparison. In E. G. Carayannis (Ed.), *Encyclopedia of creativity, invention, innovation and entrepreneurship* (pp. 1–8). New York: Springer. https://link.springer.com/referenceworkentry/10.1007/978-1-4614-6616-1_200083-1.

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "Quadruple Helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46* (3/4), 201–234. http://www.inderscience.com/browse/index.php?journalID=27&year=2009&vol=46&issue=3/4 and http://www.inderscience.com/search/index.php?action=record&rec_id=23374&prevQuery=&ps=10&m=or.

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple Helix, quadruple Helix and quintuple Helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69. https://www.igi-global.com/article/triple-helix-quadruple-helix-quintuple/41959.

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple Helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development. SpringerBriefs in business*. New York: Springer. http://www.springer.com/business+%26+management/book/978-1-4614-2061-3.

Carayannis, E. G., & Campbell, D. F. J. (2014). Developed democracies versus emerging autocracies: Arts, democracy, and innovation in Quadruple Helix Innovation Systems. *Journal of Innovation and Entrepreneurship, 3*, 12. http://www.innovation-entrepreneurship.com/content/3/1/12.

Carayannis, E. G., & Pirzadeh, A. (2014). *The knowledge of culture and the culture of knowledge. Implications for theory, policy and practice*. Houndmills: Palgrave Macmillan. http://www.amazon.de/The-Knowledge-Culture-Implications-Practice/dp/1403942439/ref=sr_1_1?ie=UTF8&qid=1403080044&sr=8-1&keywords=carayannis+knowledge+of+culture.

Carayannis, E. G., Barth, T. D., & Campbell, D. F. J. (2012). The quintuple helix innovation model: Global warming as a challenge and driver for innovation. *Journal of Innovation and Entrepreneurship, 1*(1), 1–12. http://www.innovation-entrepreneurship.com/content/pdf/2192-5372-1-2.pdf.

CNN Politics. (2016). *National president exit polls*. Atlanta: CNN. http://edition.cnn.com/election/results/exit-polls.

Danilda, I., Lindberg, M., & Torstensson, B.-M. (2009). Women resource centres. A quattro helix innovation system on the European agenda. Paper http://www.hss09.se/own_documents/Papers/3-11%20-%20Danilda%20Lindberg%20&%20Torstensson%20-%20paper.pdf.

Eigelsreiter, B. (2017). Consumerization of IT, cyber-democracy and cyber-crime: The inherent challenges and opportunities of different ends of a continuum. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Handbook of cyber-development, cyber-democracy, and cyber-defense*. New York: Springer. https://link.springer.com/referencework/10.1007%2F978-3-319-06091-0.

Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation: From national systems and "Mode 2" to a triple helix of university-industry-government relations. *Research Policy, 29*, 109–123.

Filzmaier, P., & Plasser, F. (2001). *Wahlkampf um das Weiße Haus: Presidential Elections in den USA. [Election campaign for the white house: Presidential elections in the United States.]*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Financial Times. (2017). *French election results: Macron's victory in charts*. London: Financial Times. https://www.ft.com/content/62d782d6-31a7-11e7-9555-23ef563ecf9a?mhq5j=e1.

Ghonim, W. (2012). *Revolution 2.0: The power of the people is greater than the people in power. A memoir*. Boston: Houghton Mifflin Harcourt.

Heikka, T., & Carayannis, E. G. (2016). The role of journalism in dialogic innovation processes – The case of the Helsinki Deaconess Institute multi-stakeholder workshops. *Journal of the Knowledge Economy, 7*(4), 1–27. https://link.springer.com/article/10.1007/s13132-016-0427-z.

Heikka, T., & Carayannis, E. G. (2017). Three stages of innovation in participatory journalism – co-initiating, co-sensing, and co-creating news in the Chicago school cuts case. *Journal of the Knowledge Economy, 8*(1), 1–28. https://link.springer.com/article/10.1007/s13132-017-0466-0.

Helms, L. (Ed.). (2012a). *Poor leadership and bad governance. Reassessing presidents and prime ministers in North America, Europe and Japan*. Cheltenham: Edward Elgar.

Helms, L. (Ed.). (2012b). *Comparative political leadership*. London: Palgrave Studies in Political Leadership. https://link.springer.com/bookseries/14602.

Hemer, O., & Tufte, T. (Eds.). (2005). *Media and glocal change. Rethinking communication for development*. Buenos Aires: CLACSO. http://biblioteca.clacso.edu.ar/ar/libros/edicion/media/media.html.

Hemlin, S., Allwood, C. M., & Martin, B. R. (2004). *Creative knowledge environments. The influences on creativity in research and innovation*. Cheltenham: Edward Elgar.

Kaiser, J., Fähnrich, B., Rhomberg, M., & Filzmaier, P. (2017). What happened to the public sphere? The networked public sphere and public opinion formation. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Handbook of cyber-development, cyber-democracy, and cyber-defense* (pp. 1–28). New York: Springer. https://link.springer.com/referenceworkentry/10.1007/978-3-319-06091-0_31-1.

Mitterlehner, B. (2014). Cyber-democracy and dybercrime: Two sides of the same coin. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense* (pp. 207–230). New York: Springer.

Schneider, W. (2012). *Das Ende der Angst? Die Zukunft der arabischen Welt. [The end of fear? The future of the Arab World.]*. Vienna: Braumüller.

Schneider, W. (2015). *Krieg gegen das Kalifat. [War against the Caliphate.]*. Vienna: Braumüller. http://www.braumueller.at/shop/catalog/product_info.php?products_id=2385&osCsid=6ggdphe14gblqq02rp560nu7o1&navsection=1 and https://www.youtube.com/watch?v=0mcby8LmuYo.

Spiegel Online. (2016). *Jetzt streut selbst Trump Zweifel am Wahlergebnis*. Hamburg: Der Spiegel. http://www.spiegel.de/politik/ausland/donald-trump-und-die-neuauszaehlung-jetzt-streut-selbst-er-zweifel-am-wahlergebnis-a-1123337.html.

The Telegraph. (2017a). *Macron v Le Pen: Seven charts that show how we got here – And what will happen next*. Jersey: The Telegraph. http://www.telegraph.co.uk/news/0/macron-won-first-round-french-election-will-facele-pen-second/.

The Telegraph. (2017b). *French election results: The maps and charts that explain how Macron beat Le Pen to become president*. Jersey: The Telegraph. http://www.telegraph.co.uk/news/0/french-election-results-analysis/.

U.S. Senate Select Committee on Intelligence. (2017). *Background to "Assessing Russian activities and intentions in recent US elections": The analytic process and cyber incident attribution*. Washington, DC: U.S. Senate Select Committee on Intelligence. https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

Veld, R. J. i.'t. (2010a). *Knowledge democracy. Consequences for science, politics, and media*. Heidelberg: Springer. https://link.springer.com/book/10.1007/978-3-642-11381-9.

Veld, Roeland J. in't (2010b). Towards knowledge democracy, 1–11, Roeland J. in't Veld Knowledge democracy. Consequences for science, politics, and media. Heidelberg: Springer. https://link.springer.com/chapter/10.1007/978-3-642-11381-9_1.

Wineroither, D. M., & Kitschelt, H. (2012). Die Entwicklung des Parteienwettbewerbs in Österreich im internationalen Vergleich. In L. Helms & D. M. Wineroither (Eds.), *Die österreichische Demokratie im Vergleich* (pp. 193–221). Baden-Baden: Nomos.

Xavier, R. F., & Campbell, D. F. J. (2014). The effects of cyberdemocracy on the Middle East: Egypt and Iran. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 147–173). New York: Springer. http://link.springer.com/chapter/10.1007/978-1-4939-1028-1_5.

Xavier, R. F., & Campbell, D. F. J. (2017). Cyber-democracy in the Middle East. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Handbook of cyber-development, cyber-democracy, and cyber-defense* (pp. 1–30). New York: Springer. https://link.springer.com/referenceworkentry/10.1007/978-3-319-06091-0_5-1.

Zandonella, M., & Perlot, F. (2016a). *Wahltagsbefragung und Wählerstromanalyse. BundespräsidentInnenwahl 2016*. Vienna: SORA and ISA. http://www.sora.at/fileadmin/downloads/wahlen/2016_BP-Stichwahl_Grafiken-Wahltagsbefragung.pdf.

Zandonella, M., & Perlot, F. (2016b). *Wahltagsbefragung und Wählerstromanalyse. BundespräsidentInnenwahl 2016. Wiederholung der Stichwahl*. Vienna: SORA and ISA. http://www.sora.at/fileadmin/downloads/wahlen/2016_BP-Wiederholung_Grafiken-Wahltagsbefragung.pdf.

Citizenship Education and New Media: Opportunities and Challenges

21

Maria E. Haupt

Contents

Abstract

Some decades after being introduced to all social spheres, the "new" Information and Communication Technologies (ICT) are a fixed feature in current citizenship education. This chapter highlights and discusses some of the opportunities – as well as some challenges – with regard to citizenship education and new media in formal education. Digital media, for example, offer a variety of possibilities of enhancing interactivity and of voicing one´s opinion. Additionally, citizenship education can make use of these tools by allowing for a "testing" and "trying out"

M. E. Haupt (✉)
polis – The Austrian Centre for Citizenship Education in Schools, Ludwig Boltzmann Institute of Human Rights, Vienna, Austria
e-mail: maria.haupt@univie.ac.at; maria.haupt@politik-lernen.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_1

of political action within the small scale. Still, digital media in citizenship education also bear some challenges that educators should take into account. For example, the expectation that all students – as the so-called digital natives – are competent in using digital media, may reproduce further exclusions for groups of people that don´t have access to or (yet) have the competencies of using these new tools. One major function of citizenship education therefore is to aim for the inclusion of all groups of people and to make use of all options to reach learners by the means of new media. Additionally, this chapter introduces some examples of good practice – with a focus on formal education – that make use of applying digital media within citizenship education.

Keywords

Austria · Best practices · Citizenship education · Civic education · Critical media literacy · Council of Europe · Digital divide · Digital media · Education for democratic citizenship · Formal education · Germany · Inclusive digital citizenship education · New media · Online political orientation tools

Introduction

According to Campbell (2014), the concept of Cyber-Democracy characterizes today's knowledge society. Correspondingly, the quality of democracy is closely linked to the importance that is being given to education and to fostering people's abilities and competencies to make use of the existing knowledge. Another angle refers to learners being capable of actively producing and extending knowledge themselves (Campbell 2014; Campbell and Carayannis 2014). Citizenship education aims at providing these competencies, e.g., on how to sort, analyze, and question sources of information, or how to apply knowledge to become actively involved in society. It seems reasonable to suppose that a society that is bound to become a knowledge society, may reproduce further exclusions for groups of people that don't have access to or (yet) have the competencies of using these new tools of information, communication, and participation. One major function of citizenship education therefore is to aim for the inclusion of all groups of people and to make use of all options to reach learners by the means of new media.

After a short introduction "Citizenship Education in Europe: A Brief Overview," the chapter tries to outline some of the main "Opportunities and Challenges of New Media with regard to Citizenship Education" in formal education. As critical media literacy is closely linked to citizenship education, the chapter also puts an emphasis on this learning area. To be able to provide these respective competencies, educators themselves need to be familiar with the potential and the pitfalls of digital media. Which requirements new media imply for the educators as well as the students – that for the most part are considered to be "digital natives" – is discussed subsequently. "A Selection of Examples of Best Practice on Citizenship Education and New Media in Austria and Germany" finally introduces some examples of good practice and projects in Austria and Germany – with a focus on formal education – that make use of applying digital media within citizenship education.

Citizenship Education in Europe: A Brief Overview

Giving a comprehensive overview of the topic of citizenship education in Europe is quite difficult, as the implementation, approaches, and emphases on citizenship education differ quite a lot, depending on the region, or even the country. Additionally, keeping track of the different terms that are used to describe the topic is quite a challenge, as many of the definitions are used interchangeably, while some might implicate different approaches to citizenship education (Dürr (2011) mentions, among others, "Citizenship Learning," "Democracy Learning," "Education for Democracy," "Active Citizenship," etc. For more information on these different approaches as well as a discussion of "Civic Education" and "Citizenship Education," see also Nonnenmacher and Widmaier (2011). To provide consistency, the author will stick to the term "citizenship education" throughout this chapter.). However, Dürr (2011) identifies among other commonalities one main aim of citizenship education in "most European countries," namely, "providing current and future citizens with certain competencies that enhance their democratic attitudes as well as their ability to take action and to actively participate" in democracy and society (Dürr 2011, p. 15; translation by the author; original quote in German language: "[Demnach soll CE] den jetzigen und zukünftigen Staatsbürgern bestimmte Kompetenzen vermitteln, die Entwicklung demokratischer Einstellungen fördern und Handlungsbefähigung ermöglichen bzw. zur aktiven Partizipation anregen.").

In 1997, the Council of Europe initiated the program *Education for Democratic Citizenship* (EDC), which subsequently led to a broad discussion about the principles and understandings of citizenship education in the European countries (Dürr 2011). Another important document with respect to citizenship education is the Council of Europe's *Charter on Education for Democratic Citizenship and Human Rights Education*, which all the member states agreed on in 2010. Regarding citizenship education and human rights education in formal education and vocational education, the charter states inter alia:

> Member states should include education for democratic citizenship and human rights education in the curricula for formal education at pre-primary, primary and secondary school level as well as in general and vocational education and training. Member states should also continue to support, review and update education for democratic citizenship and human rights education in these curricula in order to ensure their relevance and encourage the sustainability of this area. (Council of Europe 2010, p. 11)

Since the adoption of the charter, the member states have made an effort to implement the program and take into account the charter regarding national curricula and national strategies on citizenship education (Albeit, according to Dürr (2011), to varying degrees. Additionally, a network of EDC/HRE-coordinators aims at supporting the bi- and multilateral exchange as well as the implementation of EDC/HRE in national policies (http://www.coe.int/en/web/edc/edc/hre-coordinators). Two other influential networks striving to promote joint programs and encouraging the exchange of best practices on citizenship education and human rights education in Europe are *DARE – Democracy and Human Rights Education in Europe*

(http://www.dare-network.eu/) and *NECE – Networking European Citizenship Education* (http://www.bpb.de/veranstaltungen/netzwerke/nece/). Information on the implementation of and the different approaches to citizenship education throughout Europe in detail can be found in: Education, Audiovisual and Culture Executive Agency (Ed.) (2012): Eurydice. Citizenship Education in Europe: http://eacea.ec.europa.eu/education/eurydice/documents/thematic_reports/139EN.pdf. For more information about the history of formal citizenship education in Austria, see e.g. Wolf (1998). For more information about citizenship education in Germany, see e.g. Sander and Steinbach (2014).). At the same time, the European integration within the European Union might bear the chance to take a serious step toward a European public sphere and the development of European citizenship competencies, while building up on the consensus reached within the EDC program (Dürr (2011) mentions in this regard the European Union's program "Europe for Citizens" as one major contribution. For an in-depth discussion about the accomplishments reached so far as well as the obstacles and challenges, see Dürr (2011). For a discussion about the potential of "Creating a (European) Public Sphere" via the means of ICT-based communication, see Diecker and Galan (2014). For a discussion about "Media Education as Part of Global Democratic Citizenship Education," see Stoddard (2014).).

Opportunities and Challenges of New Media with regard to Citizenship Education

The following section focuses on the impact that the so-called new media have with regard to citizenship education. It aims at illustrating the opportunities (e.g., easier access to information and public services, enhancement of transparency, new possibilities for participation, and mobilization) as well as the challenges (e.g., the important role of critical media literacy, a possible digital divide) that digital media may imply for citizenship education (For an in-depth discussion about the advantages and challenges of Cyber-Democracy, see e.g., Barth and Schlegelmilch (2014).). Subsequently, the section outlines some of the (new) requirements for the educators as well as (new) requirements for the learners that the integration of new media into citizenship education necessitates.

Citizenship Education and the Media: An Interrelation

Mass media in general are essential for political communication, the creation of public spheres as well as the information-exchange between policy makers and the public – and vice versa. Politicians, interest groups, NGOs, and all of those who participate in political processes use the media for their purposes and for spreading their opinions and messages. At the same time, media producers function as control bodies for political actors and institutions by questioning their actions and challenging their messages as well as by contributing to the formation of opinion themselves (Kreiner 2002; Hiebl 2009). The majority of citizenship educators agree that it is

essential for citizenship education to discuss questions such as the "construction" of media and its messages as well as the implications and influences media have with regard to politics (Kreiner 2002; Hiebl 2009). Another important aspect of citizenship education is to outline the possibilities that media offer to engage oneself and to voice his or her opinion on social and political questions (Hiebl 2009). Citizenship education and the media are also closely linked, because the teaching aims at addressing and analyzing current issues and debates that are represented in the media. Moreover, the access to different types of information and various sources is crucial for the teaching of citizenship education (Overwien 2011).

The term "new media" is rather blurred, as it has been used variously over the course of time when new technologies were first being introduced (e.g., the radio was also considered once "new media"). Nowadays, the term "new media" is primarily associated with web-based digital media, such as blogs, wikis, chat forums, social networks, online games, etc. According to Besand (2005), digital media are characterized by three main functions: media integration, dynamics, and interactivity. Today, the internet allows for the access to and the integration of newspaper texts and books, offers the possibility to listen to the radio online or watch and share videos, and so on. The digitalization of media also leads to an acceleration of communication, which according to Besand (2005) is the basis for interactivity and is considered the most influential change initiated by new media. Interactivity also refers to the so-called *Web 2.0* that describes a shift from the "read-web" to the "read-write-web" (Overwien 2011). Tools like Wikipedia, YouTube, or social media allow for users not only to consume but also to produce content and to engage and exchange with other users (Overwien 2011; Maier-Rabler et al. 2012).

With regard to active citizenship, these new media have the potential to form counterpublics – in addition to, or even against the traditional and established media – that challenge dominant narratives and foster transparency by introducing differing and diverse opinions and views. As these types of media are also organized less hierarchically and offer relatively easy access, many users can contribute information and voice their opinion. Because of that, some scholars even hoped that the Web 2.0 could lead to a democratization of societal and political communication and would contribute to the inclusion of marginalized groups and minorities (Harth 2000). While there are a few studies on this subject yet, some suggest, that the disparity continues within digital media and that power structures remain intact. The theory of the *digital divide* also indicates that digital media perpetuate and reinforce existing inequalities (Weinmann 2002; Kahne et al. 2012; Maier-Rabler et al. 2012; Stoddard 2014). People with lower income and lower education are less likely to have Internet access and if they have, they use the Internet less frequently. Accordingly, they have less expertise in dealing with the new media and its opportunities, which in turn can affect their chances at school or in the labor market (Ragnedda and Muschert (2015, p. 2759) refer to this dynamic as "a recurring cycle between social and digital inequalities."). Particularly with respect to the importance of education and knowledge within the knowledge society, these discrepancies may exacerbate social differences even more (Kubicek 2002; Maier-Rabler et al. 2012; Ragnedda and Muschert 2015).

New Media in Citizenship Education: Being a Topic and Being a Tool

There are two main means to integrate digital media into citizenship education: Firstly, digital media can be addressed as a *subject/topic* for analysis in the classroom, e.g., teachers can provide insight into the formation process as well as the production conditions of messages and opinions within new media and discuss their impact on politics and society. The second way of dealing with new media is to use them as a *teaching tool* or method (Besand 2005). Teachers may include digital media into their lessons to strengthen the students' learning motivation and to be close to the young people's lives, as some studies suggest that most students appreciate it being able to use and experience digital media and discuss current topics in school (Bennett et al. 2008).

Most scholars agree that the analysis as well as the application of new media in citizenship education require for *(critical) media literacy*. Baacke (1998, quoted from Frech 2002) points out four main categories of media literacy. Firstly, students ought to get to know the media system and its providers and learn about the functions of the media (*media knowledge*). This includes taking an insight into production processes and news selection of media outlets and information providers, or have a look at access numbers and different legal conditions for media in different countries (see also Kreiner 2002). Secondly, learners should be encouraged to analyze media and its messages, its impact on politics and society, discuss the importance of independent media, changes within the media system, etc. (*media criticism*). This includes, e.g., discussing the fact that media and its technologies cannot be regarded as merely "neutral" providers of information, but may themselves take a position and have an agenda. A point of discussion may also be (power) concentration in the media as well as the question, if and which regulatory mechanisms for new media might be needed. Censorship could also be a starting point for reflections in this regard (Stoddard 2014). Another aspect may be analyzing the ways that media can contribute to constructing or deconstructing prejudices or learn about manipulative techniques that may be used by media providers (Kreiner 2002). The third category of media literacy, according to Baacke, refers to being able to make sensible use of today's media offers, e.g., being able to navigate through the multitude of information and providers, being capable of classifying various suppliers and sources and selecting the most suitable or reliable offers for each purpose (*media usage*) (see also Frech 2002; Besand 2005). Finally, being able to create and provide media (messages) oneself and being able to actively and critically participate in politics and society via the media, refers to the fourth facet of media literacy (*media creation*) (see also Frech 2002; Kahne et al. 2012).

According to Besand (2005), digital media as tools and mediators qualify for a series of activities with regard to citizenship education (The structure below also taken from Besand (2005).):

(1) Research: The web offers a multitude of information on political questions, points of views, statements, programs of political parties, and other actors that are easily accessible.
(2) Communication: Students can address (political) actors via E-Mail, Chat, Twitter, Facebook, etc. and engage in discussions about social and political questions

with the possibility of getting an instant reaction or feedback to their questions. Digital media also allow for building (interest) groups or communicating with like-minded people across regional or national borders.

(3) Simulation: Web-based online games or simulation games allow students to "try out" and practice political action with "low risk," respectively without having to fear social "sanctions" in real life (see also Middaugh and Kahne 2013) (Playful learning and model-based-learning is an approach often used in current citizenship education. It is close to the students' way of living, as many young people play (online) games on a regular basis. Computer-based simulation and experimental games furthermore allow for illustrating complex political or social scenarios and outlining causes and effects (Latsch-Gulde 2000). They offer the possibility to link theoretical knowledge with concrete actions as well as to "try out" options for action and to learn from "a model." Users can play through the different consequences of decisions they take without risking sanctions in "real life" (Schwägerl 2000; Middaugh and Kahne 2013). Players are also able to revise and adapt their actions in order to solve a problem or reach certain goals and analyze the various outcomes their actions prompt. Experiencing that one's actions have an impact on the balances of power and on our surroundings is one crucial lesson in citizenship education, which can be practiced on a small scale here. Additionally, during the game the players are confronted with the diverse and differing opinions and needs of their fellow players and are encouraged to strive for solutions and/or collective decisions (Gordon and Baldwin-Philippi 2014; Stoddard 2014). Therefore, by playing these games, the learners en passant train competencies such as "planning and taking decisions, disposing and organizing, communicating and cooperating, reasoning and negotiating, analyzing problems and finding solutions" (Klippert 1996, p. 20; quoted from Schwägerl 2000, p. 171; translation by the author) and many more, all of them being important with regard to citizenship education. However, Middaugh and Kahne (2013) underline the fact that there are not yet enough studies available to support all of these assumed potentials of online games with regard to citizenship education. Some games might also bear the risk of providing scenarios that are not complex enough or that offer solutions that are "too easy." Therefore, these games would have to be assessed and analyzed continuously to validate their usefulness.).

(4) Practicing: Learning games and online tools can contribute to gaining knowledge and expertise on topics with regard to citizenship education in a "playful manner."

(5) Doing research: There are quite some programs that support students in conducting surveys, interviews, or polls, whose results can be used for further discussion in the classroom.

(6) Production and presentation: Digital media facilitate the production of multimedia presentations and the processing of research results.

From consumers to prosumers: One major contribution of new media is, as already mentioned above, that it provides students with the opportunity to engage

as media producers themselves. This means they are not bound to being "passive" consumers, but can share information and express their opinions quite easily. That is why some scholars even coined the term of new media being possible "participation machines" (Besand 2014) (Others argue that these kinds of online participation would also require for an audience, respectively for having an impact on the public sphere, to be defined as "political participation." For more information on this discussion, see e.g., Rheingold (2008).).

Learner-centered didactics: The integration of digital media also initiated a shift toward student-centered teaching, as it allows for more autonomous and individual learning processes and enhances the students' self-appropriation of knowledge and skills (Bennett et al. 2008; Manzel 2008; Seipold 2008). Some studies even indicate that participatory and more "open" learning environments contribute to better learning outcomes with regard to citizenship education (Bennett et al. 2008). All these new opportunities at the same time bear some challenges that have to be addressed in the teaching of citizenship education.

New Requirements for Learners

One major challenge for the students is the mass of information and knowledge available via the web. They have to acquire skills to be able to sort, select, and classify complex information and practice their competence in judgment regarding the importance, reliability, and seriousness of information and sources (Weinmann 2002; Besand 2005). Digital media also prompted a shift from a primarily text-based discussion of topics with regard to citizenship education, to a gradual integration of various forms of messages, such as videos, photos, cartoons, memes, etc., that need to be addressed in citizenship education (Besand 2014). Bennett et al. (2008) stress the fact that even though most of the students – as a generation of so-called digital natives – are familiar with the use of new media, teachers should not expect every student to be competent in using digital media. This assumption could lead to students already lacking expertise in using these tools to be left even further behind. (The term "digital natives" describes the generation born after the year of 1980, in which the majority of people grew up – and is familiar – with using digital media and technologies such as the internet, computer games, smart phones, etc. At the same time, "digital immigrants" refers to users that got familiar with digital media and technologies only as adults (Maier-Rabler et al. 2012).)

What additionally characterizes the didactics of citizenship education with regard to new media is the fact that all considerations are constantly being overtaken by new technological innovations and developments. Consequently, what citizenship education demands for the most is the acquisition of skills and critical media literacy that enable students to apply their knowledge and experiences to different kinds of media – even to media that are just developing yet (Weinmann 2002; Rusch 2008; Seipold 2008).

New Requirements for Educators

Teaching in an environment in which a vast number of information is available through the web, which also can be accessed fairly quickly, teachers lose their authority of being the main providers of information and knowledge. Some scholars even suggest that their profession is transforming gradually to being primarily "guiders" through the students' learning process (Seipold 2008; Kalantzis and Cope 2010) (For an in-depth discussion about the concept of "Learning by Design: a vision for new learning," see Kalantzis and Cope (2010)). In any case, the integration of new media into citizenship education will have consequences for the learning processes, e.g., students will get different and individual results when investigating issues through web research. As another example, it may not be possible for all students to edit a video at the same time and so on (Besand 2005), which means that teachers ought to prepare for supporting their students in acquiring skills and competencies more autonomously, as well as supporting them in reaching their individual learning goals. Additionally, the integration of new media into lessons of citizenship education might require some extra effort, as it may be for example more complex to arrange for a Skype-Interview with a political activist, than stick to a "traditional" lecture on a specific topic (Rusch 2008) (Obviously, the integration of digital media requires for an adequate (technical) infrastructure. Besand (2014) recommends using low-threshold access to digital media, such as tablets or smart phones, as they make it easier to discuss and reflect the results in class, which is essential for the didactics of citizenship education.). What most authors agree on is the fact that it is crucial that teachers themselves are experienced with using digital media and stay up-to-date regarding new technologies and their possibilities (Kalantzis and Cope 2010).

According to Bennett et al. (2008), another contribution of educators with regard to new media could be to expand their concept of citizenship and participation. If educators still primarily focus on "traditional" forms of participation, they might miss out on opportunities that new and alternative forms of participation – supported by digital media – may provide (For an in-depth discussion about the two prevalent paradigms of the "disengaged youth" vs. "new forms of participation," see e.g. Bennett (2008).). Rheingold (2008) as well as Middaugh and Kahne (2013) emphasize the fact that educators could also support learners in "developing a public voice." Digital media within citizenship education should not result in creating a series of digital media products without having any impact. Using digital media to select and share information and to discuss one's opinion is one crucial lesson of (digital) civic learning. Consequently, teachers could also support students in practicing how to address "bigger" audiences, respectively reaching out to (local) institutions and getting involved within (local) communities, contributing to young people having a societal and political impact (Levine 2008; Rheingold 2008) (Concerning the much-discussed issue of the extent and the classification of young peoples' (online)-participation see also Levine (2008), Rheingold (2008), and Stoddard (2014). For a further discussion about the limitations, school structures may imply with regard to students' participation, see Middaugh and Kahne (2013).).

A Selection of Examples of Best Practice on Citizenship Education and New Media in Austria and Germany

The following section introduces some examples and projects in citizenship education, which integrate or make use of digital media. Most of them build up on, respectively take into account the considerations and observations discussed on the previous pages "Opportunities and Challenges of New Media with regard to Citizenship Education." Again, the emphasis is on projects and initiatives that can be applied to and/or are used in formal education. Most of the initiatives presented here provide accompanying learning material or information on how to make use of these offers within lessons of citizenship education. Many, however, may obviously also be of good use in extracurricular citizenship education. As the author is based in Austria, and therefore particularly familiar with projects in the German-speaking field of citizenship education, this section focuses on introducing initiatives and best practices in Austria and Germany (Many thanks to Patricia Hladschik, Sabine Liebentritt, and Elisabeth Turek (*polis* – The Austrian Centre for Citizenship Education in Schools/ Ludwig Boltzmann Institute of Human Rights) for their input and further additions with regard to the examples of good practice. For more examples of good practice as well as regular updates and new projects, see e.g., German Federal Agency for Civic Education: http://www.bpb.de, Information Portal for Citizenship Education Austria: http://www.politische-bildung.at, Information Portal for Citizenship Education Germany: http://www.politische-bildung.de or *polis* – The Austrian Centre for Citizenship Education in Schools: http://www.politik-lernen.at.).

Discussion- and Best Practice-Platforms for Educators on Digital Education

As citizenship education and (critical) media education are closely linked, the German Federal Agency for Civic Education dedicates an own platform to the topic of **Digitale Bildung in der Praxis** (*Digital Education in Practice*) (http://werkstatt.bpb.de). It allows for educators to inform themselves as well as to discuss and try out new methods and approaches. The site also comprises pro- and cons-debates and interviews with experts as well as the discussion of best practices on topics, such as "digital history-telling," "digital didactics," or the "culture of sharing in digital age." One priority is to interact with the educators and to draw on their experiences and their assessment of the methods and tools that are being introduced. In 2016, the editors and educators took up current issues, such as how to ensure quality-standards for "Open Educational Resources." One focal point was also the discussion about the possible contribution of digital citizenship education with regard to the inclusion of refugees. Another emphasis in 2016 referred to the question of how to make good use of digital games in citizenship education. The German Federal Agency for Civic Education also offers a platform called **Spielbar.de** (http://www.spielbar.de). The site introduces and assesses computer and online games and provides didactic guidelines and recommendations for parents and educators. Educators can also turn to the site of **mediamanual.**

at (http://www.mediamanual.at), provided by the Austrian Federal Ministry of Education, which offers expert articles and information on a variety of topics, such as integrative media work and media literacy. Moreover, the site provides didactic examples, best practice projects, and e-lectures (Additionally, citizenship education providers, such as the German Federal Agency for Civic Education or the Austrian Society for Citizenship Education (*Österreichische Gesellschaft für Politische Bildung*), increasingly use tools like online-courses and web-based seminars ("Webinar," MOOC) or TED-Talks for initial and further training of educators, trainers, and multipliers in citizenship education.).

Inclusive Digital Citizenship Education

The prevalence of digital media in political communication and political information bears the risk to "leave behind" those who are not (yet) equipped to use these new technologies and communication systems. At the same time, using digital media offers some possibilities to "reach" new groups of people that were not included within social and political debate sufficiently before. The following selection of examples tries to outline some of the chances digital media may provide for different groups of learners. One obstacle for people participating in political and social debate is political language being too officialese and complicated. This affects children and young people as well as people still learning the language, or people with reading difficulties (Kellermann 2014). The following Austrian and German projects are trying to support these groups in being able to join the political debate and to get to know the political system as well as one's possibilities to engage. One of these offers is provided by the **Demokratiewerkstatt** (*Democracy Workshop*) (http://www.demokratiewebstatt.at), initiated by the Austrian Parliament. Besides offering workshops, guided tours or discussions, and online-chats with members of the parliament for children and youth, the associated online-platform contains a multitude of information on political issues in child-friendly and easy-to-understand language. The site for example allows for children to draft their own law through an online-"law-generator-program" or to plan a week "being a politician."

The site **Hanisauland** (*Hipharpigland*) (http://www.hanisauland.de), implemented by the German Federal Agency for Civic Education, aims at providing political information for children aged 8–14 (The name of the platform Hipharpigland is inspired by the animals living in this fantasy state: hippos, hares and pigs.). Besides an encyclopedia on political terms and issues, the platform also offers a variety of possibilities for young people to browse and discover the site by themselves, while being in a "safe space," as the editorial board moderates the comments and the interaction on the site. A series of comics, that is also available as videos and audios, explains the functioning of democracy in a child-friendly language.

The Austrian **Politiklexikon für junge Leute** (*Online-Encyclopedia for Young People*) (http://www.politik-lexikon.at), initiated by the Austrian Ministry of Education, is another information-platform providing information on Austrian, European, and international politics as well as social and economic issues in intelligible language.

The lemmas are authored by a political scientist – which ensures the balance and quality of the information – and are updated on a regular basis. This meets teachers' demand for "high quality" educational material (For more information on this discussion, see e.g. Schuwer et al. (2014).). Furthermore, the comprehensibility of the keywords was tested with teachers and students (Ausserer et al. 2013).

The project **PoliPedia** (http://www.polipedia.at), provided by the Democracy Centre Vienna, is designed as a multimedia Online-Wiki on political issues. It allows for young people to produce their own content – "being prosumers, not only consumers," – to discuss other people's contribution and to add pictures, videos, audios, and other documents on topics like "social security," "censorship and authorship," etc. When contributing to the Wiki, users get familiar with current political topics, at the same time practice their media literacy competence, and learn how to express their opinion on social and political issues (Maier-Rabler et al. 2012; Banfield-Mumb et al. 2013).

The *UN-Convention on the Rights of Persons with Disabilities*, which came into force in 2008, secures the equal and barrier-free access of people with disabilities to all civil and human rights. This includes the right to information as well as the right to participate in political processes. Providing citizenship education that is accessible to all groups of people is a goal that has not been reached yet by far – however, there are some German and Austrian initiatives worth mentioning. The German Federal Agency for Civic Education dedicated an online-dossier to **Informationen in Leichter Sprache** (*Information in Easy-to-Read Language*) (http://www.bpb.de/die-bpb/informationen-in-leichter-sprache) and initiated a series of debates on the topic of **Inklusiv politisch bilden** (Inclusive Citizenship Education) (http://www.bpb.de/lernen/projekte/inklusiv-politisch-bilden) ("Easy-to-Read" language follows stricter rules than "easy" language regarding the length of the sentences, the formatting, and the use of pictures and so on. For more information on these distinctions, see e.g. Kellermann (2014).). In order to become even more inclusive and to reach a broader range of learners, in 2016, the Austrian Politiklexikon für junge Leute (see above) was enhanced by integrating lemmas in easy and easy-to-read language. These additional explanations were taken inter alia from the **Leichter Lesen Lexikon** (*Easy-to-Read-Lexicon*) (http://monitoringausschuss.at/glossar/), provided by the Austrian Monitoring Committee on the implementation of the UN-Convention on the Rights of Persons with Disabilities. Additionally, the Politiklexikon integrated lemmas from the platform **RECHTleicht.at** (http://www.rechtleicht.at), which was initiated by a member of the Austrian parliament. The site provides a lexicon on politics in easy language. Moreover, the section "party programs" provides the positions of the main Austrian parties in easy language and in a sign language version.

Innovative Projects Based on Digital Media

A series of projects and initiatives in citizenship education incorporates digital media to be close to the learners' usage behavior and to provide easy access and exchange. This section introduces some well-accepted and award-winning projects that stand

for several others. The German Federal Agency for Civic Education, as already mentioned above, offers numerous educational projects that are based on digital media, one of these being the platform **Chronik der Mauer** (*Chronicle of the Wall*) (http://www.chronik-der-mauer.de). The site functions as an introductory portal regarding the history of the building and the fall of the Berlin wall, covering the years from 1961 to 1990. Besides providing information on different periods and events, the site also introduces personal stories of people trying to flee across the border. Additionally, learners can use an App that provides an interactive map and guided tours along the remains of the former Berlin wall. Another App allows for users to inform themselves about historical events and stories with relation to the Berlin wall via "augmented reality," by offering overlays and fade-ins of pictures, videos, and information on their smartphones while discovering the town.

An Austrian project integrating digital media and citizenship education is the **Erster Wiener Protestwanderweg** (*First Viennese Protest Walk*) (http://www.protestwanderweg.at), initiated by *polis* – The Austrian Centre for Citizenship Education in Schools in cooperation with a writer of children's and youth books. The project aims at tracing resistance, protest, civic courage, participation, and solidarity in the Viennese cityscape (Ausserer and Hladschik 2015). The Protest Walk provides practical examples of events in recent history, in which people organized to fight for their interests and were able to contribute to a social and/or political change – e.g., the struggle for equal education for girls and women, for the rights of LGBTIQ, for independent radio stations or self-governed places in public space. Throughout the city of Vienna, learners – as well as tourists and passers-by – can discover more than 15 plaques that mark the different "stations" of the Protest Walk. The tables highlight these places of protest and engagement and provide mobile tags. By decoding the mobile tags with their smartphones, users are able to access the stories "behind" these struggles for change and to inform themselves about the achievements the protesters reached. The information is provided via text, pictures, video, and audio, integrating also original historical material. For teachers and educators who want to integrate the First Viennese Protest Walk into their lessons, the site offers educational material as well as work tasks for the students to participate actively in the discussion of these historical events (Ausserer and Hladschik 2015).

Migration on Tour (http://www.migrationontour.at) is another project using digital media as a means of citizenship education. The Exhibition was initiated by the Democracy Centre Vienna and the NGO Minorities Initiative and took into account the input and feedback of Austrian teachers and students during the developing process. The 14 chapters of the exhibition cover current topics and discussions, such as "Migration Stories," "Migration Timelines," "Suggested Solutions for European Policies on Asylum," and many more. In addition to the travelling exhibition, all content is made available as a web-based version that can be used in class and contains animated graphics, video portraits, accompanying material for educators, work and research tasks for students, an online-quiz for the students to self-test their level of knowledge, etc. (Deimel et al. 2014).

A much-noted Austrian initiative interlinking citizenship education with new media is the platform **neuwal** (http://www.neuwal.at). The blog was initiated in

2008 and aims at "promoting citizenship education and online-journalism." The site provides users with information on candidates and political parties' positions ahead of elections. Additionally, the editors prepare transcripts of selected television-interviews with politicians. They believe that making interviews accessible also via "a second channel" enhances the ability of users to analyze political messages and their structure, respectively relations and interconnections. Moreover, the transcripts may also be of good use for people with special needs and therefore contribute to inclusive citizenship education. As another service, the blog provides opinion polls by several polling agencies, thus making the similarities or differences in the results of these polls transparent. While the initiative is not particularly focusing on formal education, all offers are also well suited for citizenship education in class (The material provided on the site allows for e.g. analyzing with the students the subject of (election) polls (Who is providing the data? What is the size of the sample? Which methodology is used? What impact do polls have etc.?). Additionally, by providing transcripts of oral political statements, learners are able to analyze in-depth which language and phrases are used, carry out further research on what has been said etc. A tool allowing learners to design and implement their own polls is **Forschen mit Grafstat** (*Research with Grafstat*) (http://www.bpb.de/lernen/grafstat/), provided by the German Federal Agency for Civic Education.). Moreover, neuwal.at encourages interaction and political exchange and users can even sign up for receiving information via WhatsApp. Twitter, Facebook, Instagram, Soundcloud, and Youtube & Co are further tools used to distribute and discuss the information provided on the blog (Besides its online-offers, the association also implements other innovative projects such as the annual "Long Day of Politics" or a "Pop up-Store," accompanying the elections for the Austrian Federal Presidency in 2016.).

Online Vote Match and Political Orientation Tools

Another frequently used instrument in formal as well as non-formal citizenship education are online vote match and political orientation tools. In Austria, two teams of political scientists initiated the tools **wahlkabine.at** (*Polling Booth*) (http://www.wahlkabine.at) in 2002 and **Politikkabine.at** (*Politics Booth*) (http://www.politikkabine.at) in 2008. (The "polling booth" is provided by the Institute for New Culture Technologies in cooperation with the Austrian Political Science Association, the Society for Political Enlightenment (*Gesellschaft für Politische Aufklärung*) as well as the Department of Political Science, University of Innsbruck. The "politics booth" was implemented by the Platform Political Communication, based at the Danube University Krems.) In Germany, since 2002 the Federal Agency for Civic Education offers a tool called **Wahl-O-Mat** (http://www.bpb.de/politik/wahlen/wahl-o-mat/) for matching one's opinion with political parties' statements in the run-up to the elections. In contrast to other European tools, which are often called "Voting Advice Applications" (Fivaz et al. 2010), those responsible for the German and Austrian tools stress the fact that their main aim is to raise the user's interest in issue-oriented politics, rather than providing voting advice on which party the users

should vote for (Mayer and Wassermair 2010; Marschall 2011) (For an overview of vote match tools across Europe, see the platform **VoteMatch Europe**: http://www.votematch.eu). The German and Austrian providers preferring the term of users "playing" these tools, further makes this distinction explicit (Fivaz et al. 2010).

All three tools suggest a number between 25 and 40 carefully selected theses or questions on political issues and for each of these users choose to "agree," "not to agree," or "stay neutral" with. Additionally, the tools offer the possibility to weight the importance one attributes to each issue/topic. The vote match and political orientation tools compare these answers with the parties' answers regarding the issues in question. In the end, users receive each party's accordance with their own political opinion. Users also have the possibility to take insight into the detailed evaluation as well as the parties' written statements on the different issues. Wahl-O-Mat and wahlkabine.at in addition provide further information – e.g., a glossary on political issues, facts about the election and teaching material for using the tools in education (Mayer and Wassermair 2010; Marschall 2011). The number of users – 43.5 million (aggregate users until the year of 2014) for the German Wahl-O-Mat and 2.3 million (aggregate users until the year of 2015) for the Austrian wahlkabine.at – illustrates the persistent demand for educational tools like these. The Wahl-O-Mat even makes the list of the most sought-after offers provided by the German Federal Agency for Civic Education. The tool also receives quite a lot of media attention in the run-up to elections and the term "Wahl-O-Mat" was even integrated into the *Duden*, the dictionary of the German language (Marschall 2011). However, what are possible explanations for these vote match and political orientation tools being that popular?

1. Vote match and political orientation tools are regarded an alternative to commercial and mainstream media and as "neutral" by many users (Liebhart and Wassermair 2003; Mayer and Wassermair 2010). Either the tools are provided by a well-recognized institution such as the Federal Agency for Civic Education or a team of political scientists and are perceived as being independent from political parties.
2. There seems to be a need for issue-based information ahead of elections and beyond. As election campaigns and media coverage become increasingly focused on top candidates and persons, vote match and political orientation tools offer a central platform to gain information about political parties' position on factual issues (Mayer and Wassermair 2010; Marschall 2011).
3. Additionally, they might also be effective against information-overload and save users some time doing their research on parties' positions, as they spare themselves browsing through a multitude of party programs, interviews and discussions on current topics (Mayer and Wassermair 2010; Marschall 2011).
4. Vote match and political orientation tools also meet the idea of "playful learning" and being a game, rather than educational material. Users stated that they consider these tools as "being fun" and making them "curious" about the outcome (Mayer and Wassermair 2010).
5. Other reasons for the considerable interest in vote match and political orientation tools may also be attributed to the progressive dealignment, which requires voters to continuously re-check parties' positions on political issues (Marschall 2011).

Controversies about vote match and political orientation tools mainly relate to discussions about the equal treatment of parties and the institutional background of the supporting organization as well as transparency and quality assurance of the methodology and the evaluation (Fivaz et al. 2010). One means to strengthen users' trust in the tool is to provide as much transparency as possible. Wahlkabine.at e.g. discloses information on each round's editorial team and its methodology and evaluation-process. Additionally, the site provides strong data protection, such as not saving or forwarding users' IP addresses or other related information (Mayer and Wassermair 2010).

Initiatives Supporting Active Participation of Young People in Society and Politics

Multiple projects in citizenship education aim at providing young people with a platform to participate actively in society and politics and to have the possibility to voice their opinion on issues that are of importance to them. The following section highlights some of these platforms that stand for several others, one of these being the **No Hate Speech Movement** (http://www.nohatespeechmovement.org) (Except for the project "Young Ideas for Europe," the examples being introduced in this section do not primarily focus on formal education, but rather youth participation in general. However, they can of course be adapted for and made use of in lessons of citizenship education. Most of these projects also include a European dimension.). One major downside accompanying the regular use of digital media relates to hate speech online, which affects a growing number of internet users. To combat hate speech with regard to all spheres and tools of digital media, in 2012 the Council of Europe initiated this movement, which is since being driven by young people all over Europe. It aims at raising awareness and mapping hate speech ("Hate Speech Watch") as well as speaking up against acts of hate speech online. Additionally, the initiative provides material and resources for formal and non-formal education, such as "Bookmarks – A manual for combating hate speech online through human rights education" (Keen and Georgescu 2016), which was also translated into German language recently. The campaign integrates all sorts of digital media, such as Facebook, Twitter, YouTube, and Instagram, in which users e.g. share their photos and videos "for human rights online" – a red heart being the initiatives' catchy symbol. Many young people took up the idea of the No Hate Speech Movement and applied it to even more specific topics, one example being **Game Over Hate** (http://gameoverhate.digitalyouth.at), aiming at contributing to a nondiscriminatory and more inclusive gaming environment. Another tool integrating digital media to enhance youth participation is the so-called **Structured Dialogue** (*Strukturierter Dialog*) (http://www.strukturierter-dialog.at, http://www.strukturierter-dialog.de) (For more information on the initiative on the website of the European Commission, see: http://europa.eu/youth/have-your-say/structured-dialogue_en). The European Union

initiated these dialogues in order to be better prepared to take into account young people's views regarding the European Union's policies and to draw on the knowledge and experiences young people hold. In Austria, the National Youth Council (*Bundesjugendvertretung*) leads the national working group, whereas in Germany, the task force is headed by the German Federal Youth Council (*Deutscher Bundesjugendring*). The process comprises of consultations with youth and youth organizations in all European countries, in which, e.g., youth and policy makers meet up and discuss current European topics of relevance to young people's lives. Various online tools, such as the "Online Dialogue," aiming at collecting and comprising as many ideas and visions of young people as possible, support the exchange.

Young Ideas for Europe, initiated by the German Robert Bosch Foundation, is another example of participatory youth projects integrating digital media (The project was carried out from 2008 to 2014. For more information visit the site of the Robert Bosch Foundation (http://www.bosch-stiftung.de/content/language2/html/58743_51889.asp). During the course of the project – carried out simultaneously in several European countries – the students develop their own ideas with regard to a current European issue, such as "New Energy for Europe." They discuss what they developed with students in other European countries while staying in touch via Skype, videos, and messages. That way they are able to draw on a variety of (European) perspectives and experiences. Finally, the students' recommendations are presented to and are discussed with high-ranking policy makers in the respective fields (Another program allowing for students and teachers to get in touch with other schools and exchange on best practices (in citizenship education) via digital media is **e-Twinning** (http://www.etwinning.net), which is part of the European Union's Erasmus+-Program for "education, training, youth and sport in Europe" (http://ec.europa.eu/programmes/erasmus-plus).).

A series of participatory online youth magazines offer further possibilities to express one's opinion, to gain experience on how to "develop a public voice" (Rheingold 2008), and to practice how to engage in public discourse. In Austria, one of these being the initiative **Youth Reporter** (http://www.jugendportal.at/youth-reporter), which supports young people in being able to publish and publicly discuss their views on a series of social and political issues. The project is provided by the *Bundesnetzwerk Österreichische Jugendinfos*, the national umbrella association of the Austrian Youth Information Centers. Experienced journalists support the prospective young journalists with information and advice. A similar project implemented in Germany is **YouthReporter.eu** (http://www.youthreporter.eu), provided by *JUGEND für Europa*, the German National Agency for the EU's Erasmus+ YOUTH IN ACTION program. The platform offers the possibility for young people to exchange experiences of traveling, working, or living "abroad" in other European countries – e.g., studying abroad or completing a European voluntary service (A project at the European level is **cafébabel** (http://www.cafebabel.co.uk), an independent youth magazine run by a group of young editors, available in six languages and providing insight into the topics and matters young people care for.).

Conclusion

Some decades after being introduced to all social spheres, the "new" Information and Communication Technologies (ICT) are a fixed feature in current citizenship education. They offer a variety of possibilities of enhancing interactivity and of voicing one's opinion. Additionally, citizenship education can make use of these tools by allowing for a "testing" and "trying out" of political action within the small scale, e.g., based on simulation and online games. Other advantages include being close to the learners' everyday life and way of communicating, or contributing to "playful learning." However digital media in citizenship education also bear some challenges that educators should take into account. Integrating ICT into lessons of citizenship education requires the same amount of careful preparation and follow-up processes as all other tools being used for teaching. Another challenge for educators in this regard is to stay up-to-date concerning these new technologies in order to make sensible use of their potential. Whereas digital media offer the possibility to access information quite easily, this may at the same time lead to information overload and to people being excluded of societal and democratic participation, because they lack the skills of navigating their way through this vast number of information, or do not (yet) have access to these tools. The function of citizenship education here is to foster competencies like critical media literacy and at the same time provide offers aiming at the inclusion of all kinds of different groups of learners and for people with different starting points and diverse needs.

References

Literature

Ausserer, I., Haupt, M., Hladschik, P., & Steininger, S. (2013). *Lexika im Unterricht der Politischen Bildung. Tipps und Anregungen*. Wien: Zentrum *polis* – Politik Lernen in der Schule. http://www.politik-lernen.at/site/gratisshop/shop.item/106245.html. Accessed 15 Mar 2016.

Ausserer, I., & Hladschik, P. (2015). *Erster Wiener Protestwanderweg. Begleitheft für den Unterricht*. Wien: Zentrum *polis* – Politik Lernen in der Schule. http://www.politik-lernen.at/site/gratisshop/shop.item/106168.html. Accessed 15 Mar 2016.

Banfield-Mumb, A., Heller, G., & Mayrhofer, P. (2013). Polipedia.at. Eine Online-Enzyklopädie von und für Jugendliche. In I. Ausserer, M. Haupt, P. Hladschik, & S. Steininger (Eds.), *Lexika im Unterricht der Politischen Bildung. Tipps und Anregungen* (pp. 31–36). Wien: Zentrum *polis* – Politik Lernen in der Schule. http://www.politik-lernen.at/site/gratisshop/shop.item/106245.html. Accessed 15 Mar 2016.

Barth, T., & Schlegelmilch, W. (2014). Cyber democracy: the future of democracy? In E. Carayannis, D. Campbell, & E. Panagiotis (Eds.), *Cyber-development, cyber-democracy and cyber-defense: Challenges, opportunities and implications for theory, policy and practice* (pp. 195–206). New York: Springer.

Bennett, L. W., Wells, C., & Rank, A. (2008). *Young citizens and civic learning: Two paradigms of citizenship in the digital age. A report from the civic learning online project*. Seattle: University of Washington, Center for Communication & Civic Engagement.

Bennett, L. W. (2008). Changing citizenship in the digital age. In L. W. Bennett (Ed.), *Civic life online: Learning how digital media can engage youth*, *The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning* (pp. 1–24). Cambridge: The MIT Press. https://mitpress.mit.edu/sites/default/files/titles/content/9780262524827_sch_0001.pdf. Accessed 20 Oct 2015.

Besand, A. (2005). Mit digitalen Medien lernen – Lernprodukte und Lernumgebung. In W. Sander (Ed.), *Handbuch politische Bildung* (pp. 537–546). Schwalbach am Taunus: Wochenschau Verlag.

Besand, A. (2014). Medien neu denken. Medien als Chance und Herausforderungen für den kompetenzorientierten Unterricht. In T. Hellmuth & P. Hladschik (Eds.), *Inhalte, Methoden und Medien in der Politischen Bildung. Schriftenreihe der Interessengemeinschaft Politische Bildung* (pp. 94–105). Schwalbach: Wochenschau Verlag.

Campbell, D. F. J. (2014). Cyber-Democracy. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense: Challenges, opportunities and implications for theory, policy and practice* (pp. 113–116). New York: Springer.

Campbell, D. F. J., & Carayannis, E. G. (2014). Explaining and comparing quality of democracy in quadruple helix structures: The quality of democracy in the United States and in Austria, challenges and opportunities for development. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense: Challenges, opportunities and implications for theory, policy and practice* (pp. 117–146). New York: Springer.

Council of Europe. (2010). *Council of Europe charter on education for democratic citizenship and human rights education*. Strasbourg: Council of Europe Publishing. http://rm.coe.int/16803034e5. Accessed 10 Feb 2016.

Council of Europe (Ed.) (n.d.) *Education for Democratic Citizenship and Human Rights Education (EDC/HRE). EDC/HRE Coordinators*. Retrieved from http://www.coe.int/en/web/edc/edc/hre-coordinators. Accessed 10 Feb 2016.

DARE – Democracy and Human Rights Education in Europe. (n.d.). *About DARE*. Retrieved from http://www.dare-network.eu/about_us.htm. Accessed 10 Feb 2016.

Deimel, S., Diendorfer, G., Dorfstätter, P., Reitmair-Juárez, S., & Yann, D. (2014). *Vermittlungsprogramm zur Wanderausstellung. Migration on Tour*. Wien: Demokratiezentrum Wien. http://www.demokratiezentrum.org/fileadmin/media/pdf/MoT/MoT_VermittlProgr.pdf. Accessed 16 Mar 2016.

Diecker, J., & Galan, M. (2014). "Creating" a public sphere in cyberspace: the case of the EU. In E. Carayannis, D. F. J. Campbell, & E. Panagiotis (Eds.), *Cyber-development, cyber-democracy and cyber-defense: Challenges, opportunities and implications for theory, policy and practice* (pp. 231–255). New York: Springer.

Dürr, K. (2011). Ansätze zur Citizenship Education in Europa – Aktivitäten des Europarats und der Europäischen Union. In B. Widmaier & F. Nonnenmacher (Eds.), *Active citizenship education: Internationale Anstöße für die Politische Bildung* (pp. 13–29). Wochenschau Verlag: Schwalbach.

Education, A., & Culture Executive Agency (Eds.). (2012). *Eurydice: Citizenship education in Europe*. Education, Audiovisual and Culture Executive Agency: Brussels. https://doi.org/10.2797/83012.

Federal Agency for Civic Education. (n.d.). *NECE – Networking European Citizenship Education*. Retrieved from http://www.bpb.de/veranstaltungen/netzwerke/nece/. Accessed 29 Oct 2015.

Fivaz, J., Pianzola, J., Lander, A. (2010). More than toys: A first assessment of voting advice applications' impact on the electoral decision of voters. Working Paper No. 48. Lausanne: National Centre of Competence in Research (NCCR). *Challenges to Democracy in the 21st Century*, 1–19.

Frech, S. (2002). Medienkompetenz – nur ein Hochwert-Wort? In E. Baacke, S. Frech, & G. Ruprecht (Eds.), *Virtuelle (Lern)Welten. Herausforderungen für die politische Bildung* (pp. 149–170). Schwalbach: Wochenschau Verlag.

Gordon, E., & Baldwin-Philippi, J. (2014). Playful civic learning: Enabling reflection and lateral trust in game-based public participation. *International Journal of Communication, 8*, 759–786. http://ijoc.org/index.php/ijoc/article/view/2195/1100. Accessed 20 Oct 2015.

Harth, T. (2000). *Das Internet als Herausforderung politischer Bildung*. Schwalbach: Wochenschau Verlag.

Hiebl, E. (2009). Die Dekonstruktion der Inszenierungen. Massenmedien und politische Bildung in Gegenwart und Geschichte. In T. Hellmuth (Ed.), *Das "selbstreflexive Ich". Beiträge zur Theorie und Praxis politischer Bildung* (pp. 53–65). Innsbruck: Studienverlag.

Kahne, J., Lee, N.-J., & Feezell, J. T. (2012). Digital media literacy education and online civic and political participation. *International Journal of Communication, 6*, 1–24. http://ijoc.org/index.php/ijoc/article/view/999. Accessed 20 Oct 2015.

Kalantzis, M., & Cope, B. (2010). The teacher as designer: Pedagogy in the new media age. *E-Learning and Digital Media, 7*(*3*), 200–222. https://doi.org/10.2304/elea.2010.7.3.200.

Keen, E., Georgescu, M. (2016). *Bookmarks – A manual for combating hate speech online through human rights education*. Revised edition 2016. Strasbourg: Council of Europe.

Kellermann, G. (2014). Leichte und Einfache Sprache – Versuch einer Definition. *Aus Politik und Zeitgeschichte, 64*, 7–10. http://www.bpb.de/apuz/179341/leichte-und-einfache-sprache-versuch-einer-definition. Accessed 10 Feb 2016.

Klippert, H. (1996). Planspiele. Spielvorlagen zum sozialen, politischen und methodischen Lernen in Gruppen. Weinheim und Basel: Beltz.

Kreiner, L. (2002). Civic education and the media: theory versus practice? Observations from an ethical perspective. In Council of Europe (Ed.), *Critical approach to the media in civic education* (pp. 23–27). Strassbourg: Council of Europe Publishing.

Kubicek, H. (2002). Vor einer "digitalen Spaltung"? Chancengleicher Zugang zu den Neuen Medien als gesellschafts- und wirtschaftspolitische Herausforderung. In E. Baacke, S. Frech, & G. Ruprecht (Eds.), *Virtuelle (Lern)Welten. Herausforderungen für die politische Bildung* (pp. 53–65). Schwalbach: Wochenschau Verlag.

Latsch-Gulde, A. (2000). Mediale Lernpotenziale nutzen. Computergestützte Simulationsspiele in der politischen Bildung. In E. Bremekamp (Ed.), *Praxishandbuch Total digital + multimedial!? Impulse, Erfahrungen und Materialien für die außerschulische politische Bildung* (pp. 162–168). Schwalbach: Wochenschau Verlag.

Levine, P. (2008). A public voice for youth: The audience problem in digital media and civic education. In L. W. Bennett (Ed.), *Civic life online: Learning how digital media can engage youth*, *The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning* (pp. 119–138). Cambridge: The MIT Press. http://mitpress2.mit.edu/books/chapters/0262026341chap6.pdf. Accessed 20 Oct 2015.

Liebhart, K., & Wassermair, M. (2003). wahlkabine.at – Eine Online-Wahlhilfe erweckt neues Interesse an Politik. In S. K. Rosenberger & G. Seeber (Eds.), *Kopf an Kopf: Meinungsforschung im Medienwahlkampf*. Wien: Czernin Verlag. http://www.wahlkabine.at/ueber/literaturhinweise. Accessed 29 Jan 2016.

Maier-Rabler, U., Huber, S., & Schmid, A. (2012). Demokratieförderung durch soziale Online-Netzwerke. Politische Partizipation lernen im Web 2.0. In F. P. Bildung (Ed.), *Medien und Politik. Informationen zur Politischen Bildung Bd. 35* (pp. 17–24). Innsbruck-Wien-Bozen: Forum Politische Bildung. http://www.politischebildung.com/pdfs/35umrshas.pdf. Accessed 10 Feb 2016.

Manzel, S. (2008). *Wissensvermittlung und Problemorientierung im Politikunterricht: Lehr-Lern-Forschung. Eine anwendungsorientierte Einführung*. Schwalbach: Wochenschau Verlag.

Marschall, S. (2011). Wahlen, Wähler, Wahl-O-Mat. *Aus Politik und Zeitgeschichte, 64*, 40–46. http://www.bpb.de/apuz/33534/wahlen-waehler-wahl-o-mat?p=all. Accessed 29 Jan 2016.

Mayer, C., & Wassermair, M. (2010). wahlkabine.at: promoting an enlightened understanding of politics. In L. Cedroni & D. Garzia (Eds.), *Voting advice applications in Europe: the state of the art*. Napoli: Scriptaweb. http://www.wahlkabine.at/ueber/literaturhinweise. Accessed 29 Jan 2016.

Middaugh, E., & Kahne, J. (2013). New media as a tool for civic learning. *Communicar, 40*(*20*), 99–107. https://doi.org/10.3916/C40-2013-02-10.

Nonnenmacher, F., & Widmaier, B. (2011). Active Citizenship und Citizenship Education – Internationale Anstöße für die Politische Bildung. In B. Widmaier & F. Nonnenmacher (Eds.),

Active Citizenship Education. Internationale Anstöße für die Politische Bildung (pp. 5–12). Schwalbach: Wochenschau Verlag.

Overwien, B. (2011). Informelles Lernen in einer sich globalisierenden Welt. In W. Sander & A. Scheunpflug (Eds.), *Politische Bildung in der Weltgesellschaft. Herausforderungen, Positionen, Kontroversen* (pp. 259–275). Bonn: Bundeszentrale für politische Bildung.

Ragnedda, M., & Muschert, G. W. (2015). Max Weber and digital divide studies: introduction. *International Journal of Communication, 9*, 2757–2762. http://ijoc.org/index.php/ijoc/article/view/4424. Accessed 20 Oct 2015.

Rheingold, H. (2008). Using participatory media and public voice to encourage civic engagement. In L. W. Bennett (Ed.), *Civic life online: learning how digital media can engage youth*, *The John D. and Catherine T. MacArthur Foundation Series on Digital Media and Learning* (pp. 97–118). Cambridge: The MIT Press. http://mitpress2.mit.edu/books/chapters/0262026341chap5.pdf. Accessed 20 Oct 2015.

Rusch, G. (2008). Medienwandel zwischen Evolution und Revolution. In T. Hug (Ed.), *Media, knowledge & education. exploring new spaces, relations and dynamics in digital media ecologies* (pp. 15–35). Innsbruck: University Press. http://oapen.org/search?identifier=449459. Accessed 20 Oct 2015.

Sander, W., & Steinbach, P. (Eds.). (2014). *Politische Bildung in Deutschland. Profile, Personen, Institutionen*, *Schriftenreihe Bd. 1449*. Bonn: Bundeszentrale für politische Bildung.

Schuwer, R., Kreijns, K., & Vermeulen, M. (2014). Wikiwijs: an unexpected journey and the lessons learned towards OER. *Open Praxis, 6*(*2*), 91–102.

Schwägerl, G. (2000). "Was ist los in Neuruppern?" und "Begegnungen im globalen Dorf". Computergestützte Planspiele zum Thema "Multimedia" in der politischen Jugendbildung. In E. Bremekamp (Ed.), *Praxishandbuch Total digital + multimedial!? Impulse, Erfahrungen und Materialien für die außerschulische politische Bildung* (pp. 169–174). Schwalbach: Wochenschau Verlag.

Seipold, J. (2008). *Mobile phones in school. Selected m-learning projects from Great Britain and the German speaking countries*. In T. Hug (Ed.), *Media, knowledge & education. Exploring new spaces, relations and dynamics in digital media ecologies* (pp. 266–281). Innsbruck: University Press. http://oapen.org/search?identifier=449459. Accessed 20 Oct 2015.

Stoddard, J. (2014). The need for media education in democratic education. *Democracy & Education, 22*(1), 1–9. http://democracyeducationjournal.org/home/vol22/iss1/4/. Accessed 20 Oct 2015.

Weinmann, G. (2002). Die Neuen Medien der Informationsgesellschaft – Neue Horizonte für die politische Bildung? In E. Baacke, S. Frech, & G. Ruprecht (Eds.), *Virtuelle (Lern)Welten. Herausforderungen für die politische Bildung* (pp. 171–188). Schwalbach: Wochenschau Verlag.

Wolf, A. (1998). Zur Geschichte der politische Bildung an Österreichs Schulen. In A. Wolf (Ed.), *Der lange Anfang. 20 Jahre "Politische Bildung in den Schulen"* (pp. 7–74). Wien: Sonderzahl.

Websites of the Best Practice Projects Introduced in "A Selection of Examples of Best Practice on Citizenship Education and New Media in Austria and Germany"

café babel. European participatory magazine. Heully, A. (Executive director) http://www.cafebabel.co.uk

Chronik der Mauer (*Chronicle of the wall*). Federal Agency for Civic Education (Ed.) http://www.chronik-der-mauer.de

Demokratiewerkstatt (*Democracy Workshop*). Austrian Parliament (Ed.) http://www.demokratiewebstatt.at

Die Bundeszentrale für Politische Bildung. Informationen in Leichter Sprache (*Federal Agency for Civic Education. Information in Easy-to-Read Language*). Federal Agency for Civic Education (Ed.) http://www.bpb.de/die-bpb/informationen-in-leichter-sprache

Digitale Bildung in der Praxis (*Digital Education in Practice*). Federal Agency for Civic Education (Ed.) http://werkstatt.bpb.de

Erster Wiener Protestwanderweg (*First Viennese Protest Walk*). *polis* – The Austrian Centre for Citizenship Education in Schools (Ed.) http://www.protestwanderweg.at | http://www.politik-lernen.at/pww

e-Twinning. European Union/Erasmus+, the European Union's program to support education, training, youth and sport in Europe (Ed.) http://www.etwinning.net

Forschen mit Grafstat (*Research with Grafstat*). Federal Agency for Civic Education (Ed.) http://www.bpb.de/lernen/grafstat/

Game Over Hate. Group of young editors within the framework of the No Hate Speech Movement (Ed.) http://gameoverhate.digitalyouth.at

Hanisauland (*Hipharpigland*). Federal Agency for Civic Education (Ed.): http://www.hanisauland.de

Inklusiv politisch bilden (*Inclusive Citizenship Education*). Federal Agency for Civic Education (Ed.) http://www.bpb.de/lernen/projekte/inklusiv-politisch-bilden

Leichter Lesen Lexikon (*Easy-to-Read-Lexicon*). Austrian Monitoring Committee on the implementation of the UN-Convention on the Rights of Persons with Disabilities (Ed.): http://www.monitoringausschuss.at/glossar

mediamanual.at. Austrian Federal Ministry of Education (Ed.) http://www.mediamanual.at

Migration on Tour. Demokratiezentrum Wien and Initiative Minderheiten (*Democracy Centre Vienna and Minorities Initiative*) (Ed.) http://www.migrationontour.at

neuwal. neuwal – Verein zur Förderung der politischen Bildung und Online Journalismus (*neuwal – Association promoting citizenship education and online-journalism*) (Ed.): http://www.neuwal.at

No Hate Speech Movement. Council of Europe (Ed.) http://www.nohatespeechmovement.org

PoliPedia.at. Demokratiezentrum Wien (*Democracy Centre Vienna*) and ICT&S Center/University of Salzburg (Ed.) http://www.polipedia.at

Politiklexikon für junge Leute (*Online-Encyclopedia for Young People*). Austrian Federal Ministry of Education and Verlag Jungbrunnen (Ed.) http://www.politik-lexikon.at

Politikkabine.at (*Politics Booth*). Donau-Universität Krems (*Danube University Krems*) and Politools (Ed.) http://www.politikkabine.at

RECHTleicht.at. Kuratorium für Journalistenausbildung (*Board for Journalist Education*) (Ed.) http://www.rechtleicht.at

Spielbar.de. Federal Agency for Civic Education (Ed.) http://www.spielbar.de

Strukturierter Dialog (*Structured Dialogue*). European Union (Ed.) http://europa.eu/youth/have-your-say/structured-dialogue_en

The Austrian working group, headed by the Bundesjugendvertretung (*Austrian National Youth Council*) http://www.strukturierter-dialog.at

The German working group, headed by the Deutscher Bundesjugendring (*German Federal Youth Council*) http://www.strukturierter-dialog.de

votematch Europe. Vote Match Europe, ProDemos – House for Democracy and the Rule of Law (Ed.) http://www.votematch.eu

wahlkabine.at (*Polling Booth*). World-Information Institute. Institut für Neue Kulturtechnologien/t0 (Ed.) http://www.wahlkabine.at

Wahl-O-Mat. Federal Agency for Civic Education (Ed.) http://www.bpb.de/politik/wahlen/wahl-o-mat

Young Ideas for Europe. Robert Bosch Stiftung (*Robert Bosch Foundation*) (Ed.) http://www.bosch-stiftung.de/content/language2/html/58743_51889.asp

Youth Reporter. Bundesnetzwerk Österreichische Jugendinfos (*The National Umbrella Association of the Austrian Youth Information Centres*) (Ed.) http://www.jugendportal.at/youth-reporter

YouthReporter.eu. JUGEND für Europa (*YOUTH for Europe*) (Ed.) http://www.youthreporter.eu

What Happened to the Public Sphere? The Networked Public Sphere and Public Opinion Formation

22

Jonas Kaiser, Birte Fähnrich, Markus Rhomberg, and Peter Filzmaier

Contents

Abstract

The concepts of democracy, public sphere, and public opinion are as closely intertwined as contested. Since the dawn of the Internet, scholars have argued about its opportunities, challenges, and risks for society. Recent developments appear fundamental in that they have touched upon the core of Western

J. Kaiser (✉)
Department for Political and Social Sciences, Zeppelin University, Friedrichshafen, Germany

Berkman Klein Center for Internet and Society, Harvard University, Cambridge, MA, USA
e-mail: jonas.kaiser@zu.de; jkaiser@cyber.harvard.edu

B. Fähnrich
Zeppelin University, Friedrichshafen, Germany
e-mail: birte.faehnrich@zu.de

M. Rhomberg
Department for Political and Social Sciences, Zeppelin University, Friedrichshafen, Germany
e-mail: markus.rhomberg@zu.de

P. Filzmaier
Platform Political Communication, Danube University Krems, Krems, Austria
e-mail: peter.filzmaier@donau-uni.ac.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_31

democracies – the making of a public sphere and the forming of public opinion. The spread of digital media and changing modes of communication thus have made it necessary to reconsider classical conceptions of public sphere and public opinion. Against this background, we will posit that the emergence of the networked public sphere forces us to rethink the concepts of public sphere and public opinion in a less normative, more open, and interactive way that both is permeable to the offline world as well as to transnational demands and influences.

Keywords
Public sphere · Public opinion · Internet · Network · Democracy · Social media · Agenda setting · Climate of opinion · Mass media · Digital divide · Online communication · Fragmentation · Anonymity · Participation · Opinion leader · Spiral of silence

Introduction: Cyberspace and Public Sphere Closely Connected and Contested

When Barack Obama met Angela Merkel in 2013, the PRISM data surveillance scandal was one of Germany's most prominent and discussed issues. Germans were furious about what each new leak by Edward Snowden brought to light. Especially, the online community, the so-called netizens, demanded answers from their government and their chancellor. Merkel, during a press conference with Obama at that time, said one remarkable sentence: "The Internet is *virgin soil* for everyone of us" (Kämper 2013). What followed was the German netizens' collective malice which was quickly united under the Twitter hashtag #neuland (German for *virgin soil*) and which was picked up by journalists again to shape a debate on what constitutes #neuland – and what does not. Since then, the hashtag has transformed into a meme that is still actively used when referring to perceived ridiculous attempts to regulate the Internet or when referring to a perceived lack of knowledge about the Internet.

What some of the netizens, however, missed is that the Internet and especially its impact on society and politics and the associated societal transformations are, in fact, hardly known. In less than 30 years, the Internet has disrupted and changed nearly every aspect of our lives – both privately and politically. These changes pose huge challenges for politics and democracy. Firstly, they are especially dramatic for the legislative body and thus politicians who need to carefully weigh the pros and cons of each decision, while in the meantime online citizens adapt quickly to new practices, services, and modes of communication. Secondly, and maybe even more important, the fundaments of Western deliberation and democratic participation are heavily affected by the developments of the Internet and social media: the public sphere and the public opinion.

Although the Internet offers innumerable new opportunities, it reproduces already existing inequalities on the other: it is argued that the Internet has led toward a digital and even a possible participation divide (van Dijk 2006; Hargittai and Walejko 2008) which even widen the gap between poor and rich and uneducated and educated

citizens. Eventually, this might lead to actors that are more visible in the public, whereas those social groups who were already neglected in the political process finally become invisible.

Politics has to adjust to these developments to include not only those who are excluded but also to cater to the new demands of netizens and digital natives. New modes of political discourse require new forms of participation, new fora in which these discussions can be held and new ways of inclusion and, more drastically, concepts in which all these aspects find their places. One concept that attempts to include these aspects is the concept of the *networked public sphere* which is also connected to changes in the formation of the public opinion.

This article focuses on the intertwined connections between the concepts of democracy, the public sphere, and public opinion. The outline starts with a closer look at the classical concepts of the public sphere and the public opinion. We will then turn to the tremendous changes that both public sphere and public opinion have been facing through the Internet. Against this background, we will posit that the emergence of the networked public sphere forces us to rethink the concepts of public sphere and public opinion in a less normative, more open, and interactive way that both is permeable to the offline world and to transnational demands and influences. We will then refer to latest empirical research in the field to undermine our point of view and conclude with two perspectives which, we argue, deserve further research attention.

Democracy and Internet

The idea of democracy is a success story. It reaches back to the ancient Greece (Fleck and Hanssen 2006), and, as of now, 144 countries in the world can be described as democratic or somewhat democratic (Freedom House 2015). Many of the questions that people in ancient Greece faced are still relevant and even contested today: what constitutes a citizen; when, how, where, and even if elections are held; and how decisions are made and legitimized (Rhomberg 2008). However, there are many different answers to the very same questions which often have to do with aspects such as prevalent paradigms, epistemic research interests, socioeconomic and socio-cultural preconditions, a country's democratic "performance" (Fuchs 1998), or whether one choses to look from a normative or an empirical point of view (Lembcke et al. 2012). Accordingly, Gallie (1955) described the term democracy to be "essentially contested" already several decades ago. Hence it is mandatory to take a closer look at the different perspectives on democracy before we can focus on how and if the Internet has been challenging these ideas.

Abraham Lincoln understood democracy as "government of the people, by the people, and for the people" (qtd. in Barth and Schlegelmilch 2014, pp. 196–197). Closely connected is Schmidt's work (2013, p. 3; original emphasis) in which she defines the three principles of a democracy as "'output' *for* the people, 'input' *by* (and *of*) the people and 'throughput' *with* the people" (see also Scharpf 1997). In an attempt to find a more precise framework, Leggewie (2009, p. 73) proposes six categories as critical aspects of a democracy (see also Dahl 1989):

1. A popular government
2. Political equality
3. Democracy as political principle that spreads to other (undemocratic) systems (e.g., military)
4. Mechanism of majority
5. Moral aversion against hierarchies and arcane politics
6. Inclusion of citizens and growth of public participation

However, these categories can be interpreted in a myriad of ways. Christians et al. (2009), for example, distinguish between four types of democracy: the pluralist, administrative, civic, and direct type. They understand pluralist and administrative as "liberalism" and civic and direct as "republicanism" which both share the ideal of "deliberative democracy" (see also Trappel 2011).

Indisputably, the idea of democracy has changed with the developments of the Internet: e.g., software like LiquidFeedback or online platforms as MoveOn.org (Ito 2008; Chadwick 2007) offer more and new spaces for public participation (e.g., liquid democracy). Echoing this very idea, the former US vice president Al Gore claimed that the Internet "will not only be a metaphor for a functioning democracy, it will in fact promote the functioning of democracy by greatly enhancing the participation of citizens in decision-making" (Schulz 2011, p. 214; original emphasis). These possibilities have also influenced the way scholars viewed the impact of the Internet on democracy. Dahlberg has identified three "camps" (2001, p. 616) when it comes to democracy and the Internet in particular: the communitarian, the liberal-individualist, and the deliberative type. Whereas communitarian scholars stress the opportunities of the Internet for common interests and values, the liberal-individualist camp points to the chances which the Internet offers for the individual. Scholars favoring the deliberative model emphasize the extension of the public sphere and deliberative communication processes by online communication. Despite having different ideas regarding the change of democratic societies in Internet times, scholars of the different camps agree that the Internet will develop and most likely improve democracy. In this sense, Hagen (1997, p. 58 et seq.) differentiates between three types of digital democracies: teledemocracy, electronic democracy, and cyberdemocracy. Cyberdemocracy displays the idea that the Internet has a disruptive potential for political, economic, and social transformations. Digital networked communications are seen as a key aspect of those transformations due to their potential of avoiding centralism and fostering communities which gather around shared interests. According to Lindner (2007, p. 76), this form of democracy is marked by plebiscite elements and aims to overcome the established power structures.

So on the one hand theories of mobilization expect an increase of democratization and of democracies' quality by new information and communication technologies. On the other hand, theories of reinforcement forecast an intensification of negative developments like political discouragement, political cynicism, a culture of political mistrust, etc. At the same time politics and the scientific community are divided in "believers" and "skeptics" (for an overview of both sides, see Meckel 1999, pp. 229–243). A third group of more reserved "analysts" was only present until

the mid-1990s of the last century. "Agnostics" from the group of the so-called believers (see, e.g., Rheingold 2000) radically believe that cyberdemocracies will be the final step to implement democracy and liberalism in our society. They argue that in a cyberdemocracy every citizen will be integrated to the political process because he is able to be an active part in decision-making. "Apocalyptics" are afraid of losing quality of political information, of new forms of state control, of less personal freedom, of non-democratic elites of online information, and of a growing gap of knowledge.

Democracy and the Public Sphere

The conception of democracy has always been closely connected to the concept of the public sphere. Starting in the eighteenth and nineteenth century with the ideas of Thomas Paine and John Stuart Mill's *Considerations on Representative Government*, the question of bridging a representative parliament with its citizens via information, participation, and responsiveness became key factors in processes of democratization (Rhomberg 2009). In the early twentieth century, Lippmann (1925) and Dewey (1927) argued about the public's role and its potential in a democracy (see also Schudson 2008). Coming from a meta-analytical perspective, Ferree et al. (2002) differentiate between democratic theory on the one hand and public sphere theory on the other and conclude: "Democratic theory focuses on accountability and responsiveness in the decision-making process; theories of the public sphere focus on the role of public communication in facilitating or hindering this process" (ibid., p. 289).

The authors identify four types of democratic traditions with differing perspectives on the concept of the public sphere: the representative liberal, participatory liberal, discursive theory, and constructionist model (Ferree et al. 2002, p. 290 ff.). Whereas the representative liberal model's focus lies on the question of inclusion and especially considers the role of elite dominance (*who* is talking), the participatory model stresses the importance of empowerment within the process of public discourse (in *what* process; ibid., p. 316). For the discursive tradition, however, the most important aspect is *how* the public discourse evolves (e.g., concerning aspects such as civility and respect). For the constructionist tradition, the most pressing issue is the public discourse's outcome although this is not regarded as a final product but rather as constantly developing within the public discourse (*what* is the result; ibid., p. 317).

Probably, one of the most influential scholars when it comes to the public sphere is Jürgen Habermas whose theories clearly belong to the discursive tradition. The German sociologist has not only set the foundations for a productive but controversial debate on the public sphere. But his thoughts still inspire researchers today when it comes to understanding and conceptualizing the different kinds of public online communication on the Internet. (According to Google Scholar the German edition of his book "The Structural Transformation of the Public Sphere" has been quoted over 5,000 times and the English version over 14,000 times with over 5,000 quotes from 2011 to 2015.) In his historical analysis of democratic societies Habermas displayed how citizens left their *private* space in order to talk about political issues publically

(e.g., in coffee houses). Through this step, he argued, a bourgeois public sphere was created (Habermas) where political relevant topics were identified and disputed and a public opinion was formed. An important requirement for a functioning public sphere is the concept of deliberation, the idea that a discussion is open to everyone, equal, reciprocal, and on the basis of discursive structures. In Habermas' historical analysis, he revealed that the civil public sphere was replaced by a commercial mass media public sphere, in which media organizations and corporate interests set the agenda and framed the public discourse along economic interests (Habermas 2004).

Consequently, the ideal of an *autochthonous* public sphere (i.e., where everyone is equal) in which public opinion was formed by deliberate discussions of private citizens was replaced by a *vermachtete* public sphere (i.e., marked by power structures). This, to the contrary, was created and controlled by the mass media and in which political and economic interests had a huge impact. For Habermas, this development pushed the citizens back into the private sphere transforming them from a "Culture-Debating (kulturräsonnierend) to a Culture-Consuming Public" (Habermas, p. 159). Accordingly, the quality of the public sphere changed toward "a public sphere in appearance only" (Habermas 1989, p. 171). In his later works, however, Habermas acknowledged the importance of the mass media in the construction of the public sphere. He then regarded a free and unrestricted media system as a fundamental basis which enabled citizens to inform themselves, discuss issues, and build an unbiased (public) opinion (Habermas 1996, 2006). Only through the media could "such topics reach the larger public and subsequently gain a place on the 'public agenda'" (Habermas 1996, p. 381). With regard to the Internet, Habermas was more skeptical. His main fear was that the Internet might lead to a fragmented public sphere (Habermas 2006, 2008). But he also saw a positive impact and added that "[i]t can undermine the censorship of authoritarian regimes that try to control and repress public opinion" (Habermas 2006, p. 423).

Habermas' concept was heavily criticized for several aspects: Nancy Fraser (1990) and Chantal Mouffe (2000), for example, suggested from a feminist perspective that even though the concept of a public sphere had some merits, Habermas overlooked the issues of minorities within the political sphere and thus suggested that a normative concept should also focus on the inclusion of all voices. Fraser argued that the concept of *one* public sphere would hinder the deliberation process of minorities and thus suggested that there are in fact several "*subaltern counterpublics* [. . .] where members of subordinated social groups invent and circulate counterdiscourses, which in turn permit them to formulate oppositional interpretations of their identities, interests, and needs" (Fraser 1990, p. 67; original emphasis). The idea of a counter public or, indeed, several counter publics is also echoed by other authors who emphasize that excluded minorities both need a "safe space" to exchange perspectives and arguments but also may form coalitions with other excluded groups (cf. Warner 2005; Downey and Fenton 2003; Wimmer 2007; Nuernbergk 2013). For Craig Calhoun (1992), the weakness of Habermas' concept lies in the question of identity construction. While Habermas stated that identity building is restricted to the private sphere, Calhoun argued that this is a rather naïve idea since identities can also form and develop through participation and the forming

of communicative relationships within the public sphere since individuals also learn and ultimately change within and through public discourse.

In his later works, Habermas agreed with some of the criticism and accepted the role of counter publics that challenge the hegemony. He thus also adopted Peters' (1993) idea of *periphery* and *centrum* to his conception (Habermas 1992, 1998) and consequently understood the public sphere as being located at the periphery of the political system, transmitted by the mass media. Their task is to include all different kinds of societal actors so that all voices can be heard and a rational discourse can evolve. Habermas defined the public sphere as:

> A network for communicating information and points of view (i.e., opinions expressing affirmative or negative attitudes); the streams of communication are, in the process, filtered and synthesized in such a way that they coalesce into bundles of topically specified public opinions. (1996, p. 360)

With its emphasis on the network character of multiple issue publics in which information and opinions are being exchanged, the definition still is valid for the Internet age.

Concepts of Public Opinion

Closely connected to the development of the public sphere is the concept of public opinion that has been considered to be both a fundamental concept and "one of the fuzziest terms" (Donsbach and Traugott, p. 1) in social science research. With the diversification of media, the emergence of new forms of public engagement and the transnationalization of publics in recent years (Fraser 2007; Rhomberg 2012), defining public opinion probably has become an even more challenging task.

Whereas the origins of the term public opinion are seen in the developments of the Enlightenment, historical reviews show that public opinion as a social phenomenon has been recognized as early as in ancient Greece. In the following, several political theorists considered the influence that the public and their will might have on those in power (Price). Classical theorists such as Rousseau, Marx, Tönnies, or Habermas (to name but a few) emphasized the integrating force of public opinion as a precondition for political decision-making and analyzed grant historical changes "as their laboratories for understanding political behavior and public opinion development" (Herbst 1993b, p. 141). Common ground of these theorists was a strong normative attitude toward the concept of public opinion, its importance for (democratic) societies, and the question for the ideal relation between public opinion and government (Lazarsfeld 1957). Later on, a great part of public opinion research lost its normative tone with the raise of survey research albeit this field deployed its own political impact over time (Donsbach and Traugott). A third way of public opinion research developed in the field of communication sciences which has mainly been dedicated to the effects of mass media communication and therefore has been focusing on (empirically measurable) factors influencing public opinion (ibid.).

In accordance with the developments of the field, several attempts have been made to define public opinion. Without considering the Internet as a serious media environment yet, Herbst (1993a, p. 439) distinguished the four definitional categories "aggregation," "majoritarian," "reification," and "discursive/consensual." She considered aggregation-oriented and majoritarian concepts comparable as they inferred that "the opinions that matter are those associated with the greatest number of people" (ibid.) and thus stated that the aggregation of individual attitudes displayed the public will. "Reification" referred to theories which argued that public opinion did not exist as a real phenomenon but instead had been constructed by survey researchers, journalists, and political elites. Finally, Herbst (1993a) summarized approaches from very different paradigms in the discursive category. Definitions in this category had in common that they regarded public opinion as the result of social interaction in the public sphere. As the today maybe mostly considered theorist from this field, Habermas distinguished the public opinion from publicly articulated opinions and assumed public opinion to be the ideal result of deliberative and egalitarian publicly discussions and thus the synthesis of communication flows on a certain issue in the public sphere. Discursively and consensually oriented theorists acknowledged (albeit to a different extent and with different assessments) a certain impact of the mass media on public opinion formation. In this regard, public opinion was also associated with the opinion published in mass media (Noelle-Neumann et al. 2000). Hitherto, the assumption of a certain influence of (traditional) mass media on public opinion formation is leading the academic discourse and theory formation in communication studies and has been focus of several empirical studies in the field (Donsbach and Traugott).

New Modes of Communication and Opinion Formation in a Networked Public Sphere

Almost since the Internet's inception scholars voiced their opinions on how the Internet was going to change democracy, the public sphere and public opinion for the better or worse (cf. Filzmaier and Fähnrich). On the one side, people were enthusiastic about the opportunities the Internet had in store for civilians, minorities, the media, and the political system (e.g., Rheingold 2000; Negroponte 1995). Nicholas Negroponte (1995), for example, suggested that the future newspaper was tailored to one's personal interests ("The Daily Me"). In traditional media political discussions are characterized by a one-to-many- or few-to-many-communication. A writer of an article and a speaker on air or a small group of discussants, respectively, offer information to a mass audience. With the development of the Internet, an alternate and synchronized many-to-many-communication has become possible. Interactivity has been regarded to strengthen political discussions by supporting an interactive dialogue between government and those who are governed instead of unilateral forms of political mass communication. That is why, in the digital age, it has been argued for an improvement of public opinion formation as a main element of democratic decision-making and political participation; on the Internet not only

political elites distribute information to non-elites but "consumers" of (political) information can also be "producers" of (political) information (Rheingold 2000).

On the other side, people were afraid that through the Internet, the – already existing – gap between poor and rich, educated and uneducated, or powerful and powerless would widen even more (e.g., Putnam 2000; Sunstein 2001; Chen and Wellman 2005). Putnam (1995, 2000), for example, feared that the Internet would not lead to more participation as many hoped but rather to a phenomenon he called "Bowling Alone" which refers to the idea that users would do their own "thing" and ignore the communal opportunities the Internet offered. Hill and Hughes (1998, p. 186 qtd. in Papacharissi 2002, p. 21) remarked: "people will mold the Internet to fit traditional politics. The Internet itself will not be a historical light switch that turns on some fundamentally new age of political participation and grassroots democracy." Benkler (2006, p. 1) added to this sentiment by stating: "The change brought about by the networked information environment is deep. It is structural. It goes to the very foundations of how liberal markets and liberal democracies have coevolved for almost two centuries."

It thus becomes clear that the debates about whether the Internet fosters or hinders the development of democracy and the public sphere can be boiled down to the question of the *quality* of public communication. Neuberger (2014, p. 567) points out that the Internet influences four dimensions of public communication: the social, time, spatial, and sign dimension. There is no clear distinction between communicator and recipient anymore. A person now can both produce and use content almost simultaneously – a phenomenon which Bruns (2005) calls "produsage" (social dimension). Another aspect is that the Internet transcends the idea of "now," i.e., that users can both get immediate news updates on news sites or Twitter and search through 5-year-old forum discussions or even try to restart the discussion. The Internet is both a rapid disseminator of information and an extensive archive (time dimension). Moreover, the Internet and its decentralist architecture also have changed the way where and how we consume and produce information and how we collaborate. Journalists can, for example, work together on the same story in different locations and on different devices and yet be connected (spatial dimension). And whereas traditional news media stories were linear and confined within the spaces of a program, newspaper, or channel, the Internet allows journalists to link to other articles and websites or embed content from other sites (e.g., Tweets or YouTube videos) and by doing so soften the borders of these linear channels (sign dimensions). Neuberger adds that the Internet "simplifies reciprocal, multi-level and sequential communication" (2014, p. 567; own translation) which is in stark contrast to the traditional mass media which allow "one-sided, one-leveled and punctual communication" (ibid., p. 568; own translation) only.

Even though these changes have been visible from the beginning of online communication (e.g., via newsgroups, Usenet, forums, or mailing lists), the developments of the so-called Web 2.0 or "Social Media" radicalized these new forms of information and communication with popular services like Facebook, Instagram, Twitter, Tumblr, or Reddit (e.g., Schmidt 2013). Moreover, Castells (2007, p. 238) notes that "mass media and horizontal communication networks are converging."

Accordingly, news articles have become just one of many sources on the Internet and rival with user-generated content like blog posts, personal status updates, song recommendations, or cat pictures for the user's attention. News sites themselves provide interactive elements by adding comment sections and buttons with which the users again can share and comment the articles on different social media sites.

As several scholars have pointed out, all these changes force us to rethink the online public sphere not as one but rather as a multitude of different publics. As a result "the" public sphere is considered as a result of multiple connections and interrelations of publics which (possibly) form a technologically enabled *networked public sphere* (e.g., Castells 1996; Bieber 1999; Benkler 2006; Friedland et al. 2006; boyd 2008; Neuberger 2009, 2014; Nuernbergk 2013). (Papacharissi (2002, p. 23), for example, notes: "Our political experience online has shown that so far, the internet presents a public space, but does not yet constitute a public sphere.")

But what are networked publics? For boyd (2008, p. 38), they are "constructed through networked technologies" as well as through an "imagined collective that emerges as a result of the intersection of people, technology, and practice." According to Ito (2008, p. 2), networked publics "reference a linked set of social, cultural, and technological developments that have accompanied the growing engagement with digitally networked media." And for Benkler (2006, p. 253), the multiple networked public spheres "cluster around topical, organizational, or other common features." For Nuernbergk (2013), the networked public sphere does not replace the traditional mass media public sphere but is connected to it on different levels and touches upon other (counter-)publics and private fora. This is in line with Habermas who called the public sphere "a network for communicating information and points of view" (1996, p. 360). New, as Nuernbergk (2013, p. 146) adds, is that through the possibilities of the networked public sphere not only journalists but rather users in general are able to actively connect with each other, discuss issues, share opinions, and thus deliberately make connections visible and occasionally public (most prominently through hyperlinks but also through trackbacks on weblogs, retweets on Twitter, shares on Facebook, etc.). These connections cannot only be seen by others (e.g., search engines, web crawler, or users) but can also be used as a way of showing supposed affiliations between users. They thus emphasize the network image or metaphor in the users' mind (e.g., through network analysis or dating apps like Tinder which show the user the amount of common Facebook friends and the degree of separation).

The networked public sphere also has a big influence on journalism. Bruns (2005), for example, points out how the Internet challenges the idea of the gatekeeper (i.e., the journalist who controls which news get published and which does not) and introduces the idea of *gatewatching* which describes the collaborative attempt to find and revise news in a repetitive user-generated circle which is more of an ongoing discourse than the former "one-way" news story. In this respect, Nuernbergk (2014) emphasizes the relevance of follow-up communication as a means of connecting stories, as a "complementary relation among professional and citizen media" (ibid., p. 4). And Wojcieszak and Mutz (2009, p. 50) emphasize the potential of the often-ignored apolitical online spaces like leisure sites for political

"casual talk" and, ultimately, effective deliberation. Neuberger (2009, p. 41 ff.) concludes that the networked public sphere is characterized by the permeability of different layers of the public sphere which help to lute the breaks of the "media, formats and services" (ibid., p. 44) to improve the flow of information.

Characteristics of the Networked Public Sphere

Whereas the "classical" concepts of the public sphere and public opinion emphasize the role of mass media, the Internet as a technical environment introduced new media and different modes of communication (e.g., Facebook, Twitter, YouTube) which not only have a greater reach than traditional mass media outlets but are also heavily based on the user's active engagement. Gerhards and Schäfer (2010, p. 146) propose a model of the Internet public sphere which includes "organizational prerequisites," "openness for participation," and "impact on society" to analyze the quality of public communication on the Internet. In their study, they conclude that there is "minimal evidence to support the idea that the Internet is a better communication space as compared to print media" (ibid., p. 155). Accordingly, Zamith and Lewis identified six overarching problems or barriers which influence the formation of a public sphere and opinion on the Internet and which are regarded as useful systematization for a further outline: "a 'digital divide'; incivility among participants; the anonymity of communicators; the fragmentation of deliberation; selective exposure by individuals; and the homogenization of discussions" (Zamith and Lewis 2014, p. 4):

1. *Digital divide* describes the issue of (a) accessing the Internet and (b) using it to its potential. It thus refers to geographical, technical but also physical, educational, and societal inequalities (Hargittai 2002; van Dijk 2006). Through services like Twitter or YouTube which allow users to actively create content, the digital divide gained another facet: the digital production gap (Schradie 2011). All these aspects counter the idea that the Internet is a place of equality where everyone is able to speak their mind freely regardless of gender, ethnicity, societal or economic status, religion, or nationality but rather suggest that the Internet, too, is or can be dominated by elite voices. This is also echoed by the idea of a participation divide (Hargittai and Walejko 2008) which refers to the phenomenon that there may also be a widening gap between the people who are able to voice their opinion online through blog posts, videos, petitions, etc. and those who lack the knowledge or the mobilizing power and thus are left behind (cf. Wolling and Emmer 2014).
2. *Incivility* is a category which is closely connected to Habermas' idea of deliberation. It is based on the idea of a public discourse in Internet media which is open for everyone, where discussion is reciprocal, arguments are honest, and motivations are transparent. Questionable behavior like *flaming* or *trolling*, however, is seen by many scholars as harmful for online communities and the public deliberation processes and may indeed influence the public's perception of an issue

(e.g., Lea; Donath 1999; Herring et al. 2002; Hardaker 2010; Anderson et al. 2014). (Lee (2005, p. 385) defines flaming as "a hostile expression of strong emotions such as swearing, insults, and name-calling." And Hardaker (2010, p. 237) understands a user who trolls as "a CMC [computer mediated communication] user who constructs the identity of sincerely wishing to be part of the group in question, including professing, or conveying pseudo-sincere intentions, but whose real intention(s) is/are to cause disruption and/or to trigger or exacerbate conflict for the purposes of their own amusement." Both cases are not necessarily selective but nevertheless can be differentiated.)

3. *Anonymity* is regarded crucial for talking about one's personal opinion online or "the likelihood that individuals will engage in disruptive behavior" (Zamith and Lewis 2014, p. 4). It is unclear though whether anonymity is helpful or detrimental for the expression of opinions (e.g., Ho and McLeod 2008; Woong Yun and Park 2011). For some, anonymity offers the chance to voice opinions and experiences openly and freely without the fear of being marginalized due to one's race, gender, etc. (Binns 2012). For others, however, anonymity offers the chance to flame, troll, and harass other users (Hardaker 2010). As Santana (2011, p. 28) notes: "there is a dramatic improvement in the level of civility in online conversations when anonymity is removed."
4. Whereas some scholars were optimistic about the Internet's effect on the formation of a public sphere, Habermas (2008) warned that it would lead to its *fragmentation*. He feared that the almost infinite amount of information on the Internet would lead to a myriad of fragmented random audiences, only held together by special interests (ibid., p. 162). For him, this could lead in turn to a diffuse discourse – a "Bable objection" (Benkler 2006, p. 287; Sunstein 2001; Papacharissi 2002; Habermas 2008; Nuernbergk 2013) – where the same topics are discussed in several fraction publics with little to no exchange. Fragmentation is not limited to different websites but can also occur within one discussion thread where the discussion goes into different (partly irrelevant) directions and thus is hard to navigate and to follow (Zamith and Lewis 2014). A fragmentation of "information haves" according to issues and interests is regarded as a logical consequence. Furthermore, a general fragmentation of politically interested citizens and a loss of common requests and cohesion of solidarity and political unity might occur (ibid.). On the other hand, scholars like Fraser (1990, 1997), Mouffe (2000), or Dahlberg (2007) emphasize the need for fragmentation in order to create safe spaces for minorities where the hegemonic discourse can be criticized. Benkler (2006) acknowledges the fragmentation process, too, but emphasizes its potential for the public sphere: "the observed use of the network exhibits an order that is not too concentrated and not too chaotic, but rather, if not "just right," at least structures a networked public sphere more attractive than the mass-media-dominated public sphere" (ibid., p. 319).
5. Another important issue for online communication and the public sphere is *selective exposure*. In an *ideal* world, every user would encounter a myriad of different opinions to form his/her opinion carefully and under the impression of those diverse accounts. But there are three factors which influence information

seeking behavior on the Internet: a psychological, an algorithmic, and a social dimension. The psychological dimension refers to the idea that we rather select information which confirms our attitudes (e.g., Lazarsfeld et al. 1944; Frey 1986; Mutz 2006). Although most studies confirm that people prefer to use affirmative news, they don't necessarily avoid contradictory information (e.g., Garrett 2009). Online, however, users are hardly exposed to challenging attitudes as they can actively search for communities which reinforce their worldviews – the so-called echo chambers (Sunstein 2001; Adamic and Glance 2005). The algorithmic dimension refers to the decisions algorithms *make* for us: Facebook, for example, knows which articles we read and which we don't, which "friends" we interact with and which we ignore, and when given the information which party we usually vote for and can tell our sexuality or ethnicity by our likes (e.g., Messing and Westwood 2012; Kosinski et al. 2013; Eslami et al. 2015). This information can lead to an algorithmic generated "filter bubble" (Pariser 2011): a sphere where we only are confronted with opinions and information we agree with and which often times happens without our knowledge (Eslami et al. 2015). And Epstein and Robertson (2015) emphasize this problem by showing in several experiments that biased search engine results may in fact influence undecided voters by at least 20%. The psychological and algorithmic dimensions however are somewhat limited by the social one. This perspective refers to the institutionalized phenomenon of social recommendations by friends, communities, or user following the social web. As Messing and Westwood (2012) found, recommendations by our peers, (e.g., friends on Facebook or users we follow on Twitter) increase the likeliness that we interact with information that might challenge our views. Accordingly, the social impact can override algorithmic and psychological boundaries at least to some extent (Turcotte et al. 2015). Another study emphasized the role of those strong ties within our personal network by showing that users in a Facebook experiment were able to influence their close friends' voting decision just by posting that they already voted (Bond et al. 2012).

6. A final factor influencing the online public sphere is the issue of *convergence* or *concentration*. Whereas the fragmentation hypothesis suggests that Internet users could lose track, miss important (political) issues, and thus cannot participate in the deliberation process, the centrality hypothesis holds a different view. In this perspective it is argued that (a) even though there are millions of possible websites, only few actually are visited and thus have quasi-monopolies and (b) that in total most of the content (e.g., on blogs, microblogs, knowledge databases, comment threads, forums, etc.) is produced by few very active users which have a huge impact on the communities (Benkler 2006; Hindman 2009; Nuernbergk 2013; Zamith and Lewis 2014). Scholars thus argue that concentration processes promote homogenous debates in which most users are passive bystanders (Albrecht 2006; Dahlberg 2007). Hindman (2009, p. 55), for example, suggests that there's a "winners-take-all" phenomenon that leads to the most popular sites getting even more popular and thus forming monopolies. In his analysis he shows that the phenomenon which he calls "Googlearchy" (ibid.) is not only valid for big commercial players but also for blog networks. He thus

disagrees with Benkler (2006) who suggested that the networked public sphere would be moderately in the middle of concentration and fragmentation and thus would fulfill its role as a public sphere. In his literature review Nuernbergk (2013, p. 170 ff.) is able to show that concentration tendencies are not as tremendously as Hindman suggested and mostly apply to news and commercial sites.

As these six issues show the Internet not only changes our personal experience of how we see ourselves or others but also how we communicate; how we produce, participate, and absorb content; how we perceive and form public opinion; and consequently how we act in the public sphere.

Research Perspectives

What can be seen so far is that the perception and definition of the public sphere and public opinion have been changing due to societal changes, technological developments, and also disciplinary and epistemological viewpoints (Habermas 1989). In accordance with the changing theoretical perceptions of the public sphere and public opinion in the Internet age toward a *network concept*, it has been questioned whether these changes also can be verified empirically. In the following, we display the results of several studies of recent years which have been focusing on these questions. Most of these approaches refer to established theories of mass media research. Albeit methodological differences and difficulties in the online context (Gonzalez-Bailon and Paltoglou 2015; Emmer and Wolling 2010), these approaches are regarded useful to visualize the changes of public sphere and opinion formation which can be found alongside the developments of the (still) so-called "new" media (Woong Yun and Park 2011). Besides, researchers have found new phenomena, e.g., in the course of opinion formation in online environments which might possibly also affect the societal climate of opinion (Schulz and Roessler 2012). Concerning the quantity of empirical studies in the field, we focus our outline on four major fields that we regard as important for the purpose of our contribution. Therefore, we reflect studies referring to (1) new ways of agenda building and information diffusion; on (2) effects of online media use, agenda setting, knowledge, and attitudes; on (3) opinion formation in a networked public sphere; and (4) influencing factors on opinion formation.

New Ways of Agenda Building and Information Diffusion

Communication research has analyzed processes of agenda building and intermedia agenda setting to display the flow of information within society Boyle 2001). Moreover, the framing approach has been important to explain the influence of media on the formation of opinions. Framing analysis thus makes it possible to analyze the assessment of certain issues in media reporting by focusing on the selection and salience of certain arguments (Entman 1993; Matthes 2012). With the emergence of the Internet, it has been questioned how these theories coped with the new media environment and its possibilities of personalized information and

opinion formation (Takeshita 2006). Research focusing on agenda building has been questioning if and how the agenda of mass media differed from or was even influenced by new online media. In this regard, also the role of gate keepers and elites has been in the focus. With regard to the intermedia agenda setting of online and offline media, Ku et al. (2003) observed that journalists used online information for their inquiry and concluded that these media therefore had an impact on the agenda of mass media (cf. Sweetser et al. 2008; Winsvold 2007). Tomaszeski et al. (2009) analyzed the agenda setting function of social media, esp. political weblogs. The authors explained positive effects by the special audience of these media: the blogs were mainly considered by political journalists from traditional news media and the political elite. Whereas online media thus are considered to have a certain impact on the agenda of other media, their impact on the framing of issues seems to be limited. The results of surveys focusing on public discourses in the field of genetically modified food (Rucht et al. 2008) and human genome research (Gerhards and Schäfer 2007) indicated only minor differences regarding issues, frames, and the visibility of speakers in the online and offline debate. Wall (2006) found that weblogs on the Gulf War mainly used frames that had already been established in traditional mass media. Focusing on intermedia agenda setting effects, Chadwick (2011) describes the interrelatedness of online and offline media and argues that these connections are so strong that they need to be considered as a new "hybrid" media system in which also the influence of actors might have changed. Whereas political elites, journalists, and political activists still dominate the scene, one "should not lose sight of the fact that ordinary citizens, operating away from the elite political–media nexus, can, on occasion, affect the meaning and flow of news" (ibid., p. 19). Based on this assumption, Pfetsch et al. (2013) p. 18) question the agenda setting and framing impact that actors who neither belong to the political (e.g., governments, parliaments) nor to the journalistic system can have on the traditional mass media agenda when using online media "to assess the democratic potential of the Internet regarding its contribution to the inclusiveness of public debate." Based on previous agenda building literature, the authors argue that "effective online coalitions of challengers" (ibid.) have the power to influence the public agenda and even to trigger their issues and frames into offline media (which still define the relevance of political issues in the public sphere) and emphasize the need for further empirical research in the field. Accordingly, a study on the role of social media in the course of the Arab spring in Egypt (Meraz and Papacharissi 2013) indicates a tremendous change of journalism whereby both gatekeeping and framing work in collaboration of elites and the crowd via online media. "The findings point to new directions for hybrid and fluid journalisms that rely on subjective pluralism, cocreation, and collaborative curation" (ibid., p. 138). How fast ideas can diffuse from a rather private context toward mass media can also be demonstrated by the German debate on public sexism labeled as #Aufschrei which developed from a small Twitter conversation to a nationwide discourse within only 1 day (Maireder and Schlögl 2014). In their research centered in diffusion theory, Bakshy et al. (2012, p. 526) hint to the strength of weak ties when examining the diffusion of ideas within a social media framework. Concerning diffusion processes on Facebook, they

"suggest that in large online environments, the low cost of disseminating information fosters diffusion dynamics that are different from situations where adoption is subject to positive externalities or carries a high cost."

Effects of Online Media Use: Agenda Setting, Knowledge, and Attitudes

Whereas research on agenda building and diffusion helps to explain the flow of information within society, communication research has also focused on the effects of media use: the agenda setting-theory (McCoombs and Shaw 1972) argues that mass media have a strong impact on the (political) issues regarded important by recipients: "The media are the major primary sources of national political information [. . .] the evidence in this study that voters tend to share the media's composite definition of what is important strongly suggests an agenda-setting function of the mass media" (ibid., pp. 185, 184). This, one could conclude, is not only valid for the agenda construction of individuals but also evolves on a societal level (critical: Rhomberg 2008; Rössler 2008). With regard to possible changes in the digital world, Althaus and Tewksbury (2002) researched the agenda setting effects on the readers of the print and online version of the New York Times and in fact found differences. Reasons for the altered agendas were seen in the possibilities to control exposure in the online setting which let readers to focus on different information and also to assess the importance of issues differently. Other studies did not find significant differences in the agendas of people who get their news online and those who get them offline (for a summary Nuernbergk 2013, p. 166) and suggested a rather low fragmenting effect of online media (Coleman and McCombs 2007; Emmer and Wolling 2007) but showed that the use of online media affected the knowledge of certain issues: Dalrymple and Scheufele (2007) could show that online newspaper readers had a higher level of knowledge regarding the issues of the media agenda than offline newspaper readers and television users. Nisbet and Scheufele (2004) also found a positive correlation of the reception of online information on political campaigns and political attitude efficacy. In contrast, Muhlberger (2003) reported no significant differences regarding the effects on political attitudes and activities among traditional media recipients and online users. Accordingly, a study by Muñiz et al. (2015) on framing effects showed no significant correlation between media frames and recipients' frames as displayed in forum comments by users. Whereas these single studies might question the "real power" (ibid., p. 3257) of online media to transfer their frames directly on media users, altered modes of communication within a networked public sphere also contest traditional ideas of opinion formation. Hyperlink studies suggest that there are no truly isolated spaces but rather weaker and stronger connections between network clusters and even "divided" or polarized (counter-)publics (e.g., Adamic and Glance 2005; Nuernbergk 2014).

Opinion Formation in a Networked Public Sphere

So, how does public opinion formation work in the framework of a networked public sphere and which impact do online media have? Processes of opinion formation are in the core of the so-called spiral of silence theory (Noelle-Neumann 1984) and

related empirical research. Since its publication in the 1970s, the theory has been one of the "true macroscopic" and most discussed models explaining the making of public opinion (Scheufele 2008, p. 182; Glynn et al. 1997). The theory largely refers to social psychological concepts, especially regarding dynamics within social entities. It is assumed that people anticipate the opinions that other people have on certain issues. Due to a fear of isolation, people only speak out publicly when they are convinced that their personal opinion conforms to the majority opinion but keep silent if they expect the opposite. For Noelle-Neumann (Noelle-Neumann et al. 2000; Noelle-Neumann 1984), a dynamic process then guides the dominant opinion from the level of encounter publics to the societal level whereby a consonant mass media reporting is considered to have a strong influence on public opinion. Due to the complexity of public opinion formation, empirical research has mainly testified aspects of the model which refer to individual and intergroup opinion formation (Glynn et al. 1997). Several influencing factors were found: especially, the nature of issues and its moral component seem to be important (Scheufele 2008), the cultural setting was found to have an impact (Huang 2005), and it was indicated that personal reference groups had a higher impact on the estimated climate of opinion than the perceived public opinion expressed in the mass media (Moy et al. 2001). Moreover, attitude certainty was considered to have an impact on the willingness to speak out (Matthes et al. 2010). With the changes of information and communication practices in recent years, the model was applied to Internet and social media communication to explain the emergence of opinions in online environments and their possible impact on the societal climate of opinion. Research therefore focused on different assumptions of the original theory and let to ambiguous results: Porten-Cheé and Eilders (2015) investigated how exposure to user-generated online content affected the perceived opinion climate and the willingness of people to speak out in the field of climate change communication. Results of their diary study did not show a silencing but rather a strengthening effect to voice one's opinion: "individuals who viewed themselves as part of the minority were even more willing to speak out in public than those who viewed themselves as part of the majority" (ibid., p. 7). Moreover, exposure to user-generated content did not affect the perceived climate of opinion. Liu and Fahmy (2011) compared the willingness to speak out in online and offline settings with regard to the morally highly controversial issue of same-sex marriages. They found that people feared less isolated in an online setting but that especially the fear of suppression and attack had an impact on the willingness to speak out on the Internet. Their results also indicated a positive correlation to speak out in different environments – online and offline.

Based on the developments of a fragmented media use, individual information selection and exposure under online conditions (Putnam 2000), Schulz and Roessler (2012) questioned the original assumptions of the spiral of silence that all individuals receive the same media tone and develop the same "objective" opinion – an important precondition for the formation of a *public* opinion. Their results show that the characteristics of online communication cause more diverse selection patterns which lead to "self-constructed information *bubble(s)*" and "subjectively perceived opinion climates" (ibid., pp. 351–352). In accordance with the

fragmentation of the public sphere which can be found in developments such as filter bubbles and echo chambers (see chapter 5.1), these results link to a fragmentation of opinions in a networked public sphere.

In their study of online reader comments – one of the most popular forms of user-generated online content – Friemel and Dötsch (2015) analyzed the influence of online comments on the perceived opinion of online media users. (The text does not refer to the spiral of silence but is regarded suitable here since the authors refer to the climate of opinion – a term closely related to Noelle-Neumann et al.'s (2000) original theory and related research.) Their survey also focused on the question of who is writing and who is reading online comments in eight Swiss newspapers. They found that these groups differed significantly: writers were in average rather male, younger, and politically more right-wing oriented than readers. "Nevertheless, the published opinion in comments is regarded as a valid indicator for the opinion of news site users" (ibid., p. 165). But the results of the study also made a problematic constellation visible since neither readers nor writers of comments were aware of the bias. Whereas the study focuses on a Swiss case, it could be argued – and needs to be testified empirically – that online news site users in general consider user-generated content in online forums as a valid indicator for the opinion of all news site users or even for the *public* opinion.

Influencing Factors on Opinion Formation

Interpersonal channels have been especially considered to be effective in forming and changing attitudes toward new ideas (Rogers 2002, p. 990). Against this background, the concept of opinion leadership has become influential in public opinion research. The concept distinguishes different roles within communication processes whereby people show differences in their communicative behavior. Some are considered to provide information and give orientation, whereas others follow these leaders and their ideas. Literature on the concept shows that opinion leaders differ regarding their personality, their interest in certain issues, and also their range of activity in communicating their views (Trepte and Scherer 2010). With their multistep concept of opinion diffusion, Katz and Lazarsfeld (1955) showed far before the coming of the Internet that ideas pass within a network of communication. Several authors from both marketing (van der Merwe and van Heerden 2009; Shoham and Ruvio 2008) and communication research (Nisbet and Kotcher 2009; Trepte and Scherer 2010) have addressed the question whether changing modes of communication and the merging of interpersonal and media communication on the Internet and social media had an impact on opinion leadership. They drew very different conclusion reaching from the rising importance of opinion leaders in the virtual world of social media (Kavanaugh et al. 2006) to a decline and neglecting of their influence under online conditions (Bennett and Manheim 2006). Schäfer and Taddicken (2015) researched communicative roles on the Internet by using a survey from German Internet users. They found that the concept of opinion leadership also applies to online communication and could retrieve certain communicative roles which had been described in previous studies focusing on offline communication: the proactive opinion leader, opinion followers, and inactive respondents. A new

role model identified was the mediatized opinion leader: "They give advice to others even more often than regular Opinion Leaders and exhibit by far the strongest and most diverse use of media and communication channels. To acquire information about a topic, they use both mass media and online media significantly more often than all other groups. In their opinion leadership relations, they employ face-to-face communication, interpersonal media, and online media significantly more than all other clusters" (ibid., p. 973). The emergence of a new type of opinion leadership here again is rooted in the networked public sphere with its hybrid nature.

The new modes of online communication have also influenced the tone of communication on the Internet. Several authors therefore have focused on the effects which incivility – ranging from unrelated, rude critique to outrageous and incense claims – might have on opinion formation. In their study on incivility in the course of online discussions of nanotechnology, Anderson et al. (2013) could show that especially individuals with a rather negative attitude toward the technology are affected by incivil comments and perceive it as more risky than others who are exposed to civil comments (nasty effect). They conclude that online communication of new topics (e.g., emerging technologies) might enrich public deliberation but that incivility "may impede this democratic goal" (ibid., p. 11). Lee (2005) notes that members of online communities would form their own ways of dealing with rude online comments, e.g., withdrawal but also joking. Reader (2012) however adds that users and journalists have different perceptions of what constitutes "civility." Papacharissi (2004, p. 280) argues that incivil comments, though often reprimanded online, contest individual rights, "pose a threat to democracy and, by their very nature, thwart the development of a public sphere."

An Only Preliminary Conclusion

Undoubtedly, the last 30 years have seen tremendous changes in the ways of communication and interaction which have their reasons in the development of the Internet and social media. These changes appear fundamental in that they have touched upon the core of Western democracies – the making of a public sphere and the forming of public opinion. The spread of digital media and changing modes of communication thus have made it necessary to reconsider classical conceptions of public sphere and public opinion. Against this background, the idea of the networked public sphere was developed.

Starting with Habermas, many scholars have argued about the consequences which the developments might bring for democracy. Critical positions consider the mix of journalistic, parajournalistic, and non-journalistic issues and opinions on the web as problematic because it limits the share of qualified information and verified opinion (Donsbach 2011). Public opinion in a networked public sphere thus is argued to become rather irrational, ideological, or superficial (ibid.). Moreover, fragmentation, selective exposure, and incivility have been addressed as developments which might hinder public deliberation and democratic participation.

On the other side, these developments have been considered as the flipside of potentially positive aspects for democracies. Even though some scholars see echo chambers as something problematic, Fraser (1990) has pointed out to the need for smaller publics so that stories can be heard and opinions can be formed outside of the hegemonic opinion. The same holds true for journalism: even though the digitalization has threatened many aspects of journalism (monetization, job security, journalistic routines, reach, etc.), it has also widened opportunities to interact with the audience, to find new sources, to mix formats, and even to develop new business ideas (e.g., Buzzfeed). Benkler (2006, p. 242) has added that the "emerging networked public sphere [is] more responsive to intensely held concerns of a much wider swath of the population than the mass media were capable of seeing, and creates a communications process that is more resistant to corruption by money."

Against this background, the formation of a networked public sphere is closely connected to cyber democracy as they both emphasize the Internet's disruptive potential for political, economic, and social transformations. As Campbell et al. (2015; see also chapter 4) point out, the Internet plays a key role when it comes to fostering the "knowledge democracy." The diffusion of knowledge, information, and opinions in the networked public sphere and its impact on the quality of democracy, then, remains a highly important issue for social science research.

In fact, rather the idea of a networked public sphere nor its pros and cons are #neuland of communication research anymore. But undoubtedly, the fast developments of recent years will proceed and therefore need further attention. For us, two aspects are especially important for consideration:

1. What is the political in the new public sphere? Questions of the public sphere and public opinion have always been closely connected to the political sphere. But what, in fact, is political – and what is not? In the networked public sphere, this question has no definite answer because a major change of recent developments refers to the tension of the "private" and the "public" in media democracy. Quite often, it has been argued that online media would hardly affect political communication, opinion formation, and activity because these fields were still dominated by traditional mass media (even if in their online version) (Donsbach 2011). But cases such as #aufschrei, #Egypt, or the bullygate affair show how fast information diffuses in a hybrid media system. And they show how fast news lose their private nature and turn political so that the distinction of what is private and what is political seems to melt away. "Online media lend themselves to several uses, but they acquire agency as they enable the renegotiation of what is considered private and what is considered public in public life" (Papacharissi 2011, p. 231). Wojcieszak and Mutz (2009) suggest that the potential for deliberation on political issues online occurs mostly outside the classical political spaces. As far as issues and publics become more and more politicized, we need a new and broader understanding of the political.
2. What changes if our perceptions change? It has been outlined that the idea of the network as the frame for the public sphere has its roots in communication technology. Despite different perspectives, scholars agree that online communication as

well as its basic architecture is built on networks, networks that influence how, when, where, if, and with whom we communicate. As Friedland et al. (2006, p. 7) point out: "Networked forms of communication provide the form of connection among diverse social networks. In addition, they constitute a modality through which social relationships are created, extended, and maintained." Undoubtedly, the imagination of the public sphere as a network of several publics, situated in different locations, connected via diverse media and even linked over time is a very obvious visualization, and it is timely as it fits to the concept of the network society in which we are said to live. But could we also change this image? How could we imagine the public sphere and the formation of public opinion instead and how would this change our understanding of developments – and maybe even the modes of communication itself? Of course, these considerations lead not only to empirical but also theoretical and even epistemological questions. They show that the developments of the public sphere and public opinion bring about both theoretical and methodological challenges. From a theoretical point of view, the networked public sphere is a starting point to explain the interrelations of actors, media, time, and space. From a methodological point of view, the model is still far too complex to analyze more than just single parts. Therefore, also the use of methodology considers critical reflection.

References

Adamic, L. A., & Glance, N. (2005). *The political blogosphere and the 2004 U.S. election. Divided they blog.* Paper presented at the 3rd international workshop on Link discovery, Chicago.

Albrecht, S. (2006). Whose voice is heard in online deliberation? A study of participation and representation in political debates on the Internet. *Information, Communication & Society, 9*(1), 62–82.

Althaus, S. L., & Tewksbury, D. (2002). Agenda setting and the "new" news. Patterns of issue importance among readers of the paper and online versions of the New York Times. *Communication Research, 29*(2), 180–207.

Anderson, A. A., Brossard, D., Scheufele, D. A., Xenos, M. A., & Ladwig, P. (2014). The "nasty effect." Online incivility and risk perceptions of emerging technologies. *Journal of Computer-Mediated Communication, 19*(3), 373–387.

Bakshy, E., Rosenn, I., Marlow, C., & Adamic, L. (2012). *Proceedings of the 21st international conference on World Wide Web*. New York: ACM.

Barth, T., & Schlegelmilch, W. (2014). Cyber democracy. The future of democracy? In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense* (pp. 195–206). New York: Springer.

Benkler, Y. (2006). *The wealth of networks. How social production transforms markets and freedom*. New Haven: Yale University Press.

Bennett, W. L., & Manheim, J. B. (2006). The one-step flow of communication. *The Annals of the American Academy of Political and Social Science, 608*(1), 213–232.

Bieber, C. (1999). *Politische Projekte im Internet. Online-Kommunikation und politische Öffentlichkeit*. Frankfurt/New York: Campus.

Binns, A. (2012). Don't feed the trolls! *Journalism Practice, 6*(4), 547–562.

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature, 489*(7415), 295–298.

boyd, d. (2008). *Taken out of context. American teen sociality in networked publics*. Ph.D. dissertation, University of California-Berkeley. http://www.danah.org/papers/TakenOutOfContext.pdf

Boyle, T. P. (2001). Intermedia agenda setting in the 1996 presidential election. *Journalism and Mass Communication Quarterly, 78*(1), 26–44.

Bruns, A. (2005). *Gatewatching. Collaborative online news production*. New York: Peter Lang.

Calhoun, C. (1992). Introduction. In C. Calhoun (Ed.), *Habermas and the public sphere* (pp. 1–50). Cambridge: The MIT Press.

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493. https://doi.org/10.1007/s13132-015-0246-7.

Castells, M. (1996). *The rise of the network society*. Cambridge: Blackwell.

Castells, M. (2007). Communication, power and counter-power in the network society. *International Journal of Communication, 1*, 238–266.

Chadwick, A. (2007). Digital network repertoires and organizational hybridity. *Political Communication, 24*(3), 283–301.

Chadwick, A. (2011). The political information cycle in a hybrid news system. The British prime minister and the "Bullygate" affair. *The International Journal of Press/Politics, 16*(1), 3–29.

Chen, W., & Wellman, B. (2005). Minding the cyber-gap. The Internet and social inequality. In M. Romero & E. Margolis (Eds.), *The Blackwell companion to social inequalities* (pp. 523–545). Malden: Blackwell.

Christians, C. G., Glasser, T. L., McQuail, D., Nordenstreng, K., & White, R. A. (2009). *Normative theories of the media: Journalism in democratic societies*. Urbana: University of Illinois Press.

Cobb, R. W., & Elder, C. D. (1971). The politics of agenda-building. An alternative perspective for modern democratic theory. *The Journal of Politics, 33*(4), 892–915.

Coleman, R., & McCombs, M. (2007). The young and agenda-less? Exploring age-related differences in agenda setting on the youngest generation, baby boomers, and the civic generation. *Journalism and Mass Communication Quarterly, 84*(3), 495–508.

Dahl, R. (1989). *Democracy and its critics*. New Haven: Yale University Press.

Dahlberg, L. (2001). The Internet and democratic discourse: Exploring the prospects of online deliberative forums extending the public sphere. *Information, Communication & Society, 4*(4), 615–633.

Dahlberg, L. (2007). Rethinking the fragmentation of the cyberpublic: From consensus to contestation. *New Media & Society, 9*(5), 827–847.

Dalrymple, K. E., & Scheufele, D. A. (2007). Finally informing the electorate? How the Internet got people thinking about presidential politics in 2004. *The Harvard International Journal of Press/Politics, 12*(3), 96–111.

Dewey, J. (1927). *The public and its problems*. New York: Holt.

Donath, J. S. (1999). Identity and deception in the virtual community. In M. A. Smith & P. Kollock (Eds.), *Communities in cyberspace* (pp. 29–59). New York: Routledge.

Donsbach, W. (2011). Risiken und Nebenwirkungen des Internets für die politische Kommunikation. *Studies in Communication | Media, 1*(1), 119–129.

Donsbach, W., & Traugott, M. W. (2008a). Public opinion – A nebulous concept. In W. Donsbach & M. W. Traugott (Eds.), *The SAGE handbook of public opinion research* (pp. 1–5). London: Sage.

Donsbach, W., & Traugott, M. W. (Eds.). (2008b). *The SAGE handbook of public opinion research*. London: Sage.

Downey, J., & Fenton, N. (2003). New media, counter publicity and the public sphere. *New Media & Society, 5*(2), 185–202.

Emmer, M., & Wolling, J. (2007). Leben in verschiedenen Welten? Themenagenden von Offlinern und Onlinern im Vergleich. In S. Kimpeler, M. Mangold, & W. Schweiger (Eds.), *Die digitale Herausforderung. Zehn Jahre Forschung zur computervermittelten Kommunikation* (pp. 239–250). Wiesbaden: VS Verlag für Sozialwissenschaften.

Emmer, M., & Wolling, J. (2010). Online-Kommunikation und politische Öffentlichkeit. In W. Schweiger & K. Beck (Eds.), *Handbuch Online Kommunikation* (pp. 36–58). Wiesbaden: VS Verlag für Sozialwissenschaften.

Entman, R. M. (1993). Framing. Toward clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51–58.

Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of election. *Proceedings of the National Academy of Sciences, 112*(33), E4512–E4521.

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., & Sandvig, C. (2015). *"I always assumed that I wasn't really that close to [her]": Reasoning about invisible algorithms in news feeds.* Paper presented at the proceedings of the 33rd annual ACM conference on human factors in computing systems, Seoul.

Ferree, M. M., Gamson, W. A., Gerhards, J., & Rucht, D. (2002). Four models of the public sphere in modern democracy. *Theory and Society, 31*, 289–324.

Filzmaier, P., & Fähnrich, B. Strategische Kommunikation in der Politik. In M. Holenweger et al. (Eds.), *Strategische Kommunikation*. Baden-Baden: Nomos.

Fleck, R. K., & Hanssen, F. A. (2006). The origins of democracy: A model with application to ancient Greece. *Journal of Law and Economics, 49*(1), 115–146.

Fraser, N. (1990). Rethinking the public sphere. A contribution to the critique of actually existing democracy. *Social Text,* (25/26), 56–80.

Fraser, N. (1997). *Justice interruptus. Critical reflections on the "postsocialist" condition*. New York: Routledge.

Fraser, N. (2007). Special section. Transnational public sphere. Transnationalizing the public sphere. On the legitimacy and efficacy of public opinion in a post-Westphalian world. *Theory, Culture & Society, 24*(4), 7–30.

Freedom House. (2015). *Freedom in the world 2015*. Washington, DC: Freedom House.

Frey, D. (1986). Recent research on selective exposure to information. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 19, pp. 41–80). New York: Academic.

Friedland, L. A., Hove, T., & Rojas, H. (2006). The networked public sphere. *Javnost – The Public, 13*(4), 5–26.

Friemel, T. N., & Dötsch, M. (2015). Online reader comments as indicator for perceived public opinion. In M. Emmer & C. Strippel (Eds.), *Kommunikationspolitik für die digitale Gesellschaft* (Digital Communication Research, Vol. 1, pp. 151–172). Berlin: ifpuk – Institute for Media and Communication Studies at FU.

Fuchs, D. (1998). Kriterien demokratischer Performanz in liberalen Demokratien. In M. T. Greven (Ed.), *Demokratie – eine Kultur des Westens? 20. Wissenschaftlicher Kongress der Deutschen Vereinigung für Politische Wissenschaft* (pp. 151–179). Opladen: Leske + Budrich.

Gallie, W. B. (1955). Essentially contested concept. *Proceedings of the Aristotelian Society, 56*(1), 167–198.

Garrett, R. K. (2009). Echo chambers online?. Politically motivated selective exposure among Internet news users. *Journal of Computer-Mediated Communication, 14*(2), 265–285.

Gerhards, J., & Schäfer, M. (2007). Demokratische Internet-Öffentlichkeit? Ein Vergleich der öffentlichen Kommunikation im Internet und in den Printmedien am Beispiel der Humangenomforschung. *Publizistik, 52*(2), 210–228.

Gerhards, J., & Schäfer, M. S. (2010). Is the Internet a better public sphere? Comparing old and new media in the USA and Germany. *New Media & Society, 12*(1), 143–160.

Glynn, C. J., Hayes, A. F., & Shanahan, J. (1997). Perceived support for one's opinions and willingness to speak out. A meta-analysis of survey studies on the "spiral of silence". *Public Opinion Quarterly, 61*(3), 452–463.

Gonzalez-Bailon, S., & Paltoglou, G. (2015). Signals of public opinion in online communication. A comparison of methods and data sources. *The Annals of the American Academy of Political and Social Science, 659*(1), 95–107. https://doi.org/10.1177/0002716215569192.

Habermas, J. (1989). *The structural transformation of the public sphere. An inquiry into a category of bourgeois society*. Cambridge: MIT Press.
Habermas, J. (1990/1962). *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaften. Mit einem Vorwort zur Neuauflage 1990*. Frankfurt a. M.: Suhrkamp.
Habermas, J. (1992). *Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaates*. Frankfurt a. M.: Suhrkamp.
Habermas, J. (1996). *Between facts and norms: Contributions to a discourse theory of law and democracy*. Cambridge: Polity Press.
Habermas, J. (1998). *The inclusion of the other: Studies in political theory*. Cambridge: MIT Press.
Habermas, J. (2004). *The divided West*. Malden: Polity Press.
Habermas, J. (2006). Political communication in media society. Does democracy still enjoy an epistemic dimension? The impact of normative theory on empirical research. *Communication Theory, 16*(4), 411–426.
Habermas, J. (2008). Hat die Demokratie noch eine epistemische Dimension? Empirische Forschung und normative Theorie. In J. Habermas (Ed.), *Ach, Europa* (pp. 138–191). Frankfurt a. M.: Suhrkamp.
Hagen, M. (1997). *Elektronische Demokratie. Computernetzwerke und politische Theorie in den USA*. Hamburg: Lit-Verlag.
Hardaker, C. (2010). Trolling in asynchronous computer-mediated communication. From user discussions to academic definitions. *Journal of Politeness Research. Language, Behaviour, Culture, 6*(2), 215–242.
Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. *First Monday, 7*(4).
Hargittai, E., & Walejko, G. (2008). The participation divide: Content creation and sharing in the digital age. *Information, Communication & Society, 11*(2), 239–256.
Herbst, S. (1993a). History, philosophy, and public opinion research. *Journal of Communication, 43*(4), 140–145.
Herbst, S. (1993b). The meaning of public opinion. Citizens' constructions of political reality. *Media, Culture and Society, 15*, 437–354.
Herring, S. C., Job-Sluder, K., Scheckler, R., & Barab, S. (2002). Searching for safety online: Managing "trolling" in a feminist forum. *The Information Society, 18*, 371–383.
Hill, K. A., & Hughes, J. E. (1998). *Cyberpolitics: Citizen activism in the age of the Internet*. New York: Rowman & Littlefield.
Hindman, M. (2009). *The myth of digital democracy*. Princeton: Princeton University Press.
Ho, S., & McLeod, D. M. (2008). Social-psychological influences on opinion expression in face-to-face and computer-mediated communication. *Communication Research, 35*, 190–207.
Huang, H. (2005). A cross-cultural test of the spiral of silence. *International Journal of Public Opinion Research, 17*(3), 324–345.
Ito, M. (2008). Introduction. In K. Varnelis (Ed.), *Networked publics* (pp. 1–14). Cambridge: MIT Press.
Kämper, V. (2013). Die Kanzlerin entdeckt #Neuland. *Spiegel Online*. http://www.spiegel.de/netzwelt/netzpolitik/kanzlerin-merkel-nennt-bei-obama-besuch-das-internet-neuland-a-906673.html
Katz, E., & Lazarsfeld, P. (1955). *Personal influence, the part played by people in the flow of mass communications*. New Brunswick: Transaction Publishers.
Kavanaugh, A., Zin, T. T., Caroll, J. M., Schmitz, J., Pérez-Quiñones, M., & Isenhour, P. (2006). When opinion leaders blog. New forms of citizen interaction. In *Proceedings of the 2006 international conference on Digital government research.* Digital Government Society of North America.
Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences, 110*(15), 5802–5805.
Ku, G., Kaid, L. L., & Pfau, M. (2003). The impact of web site campaigning on traditional news media and public information processing. *Journalism and Mass Communication Quarterly, 80*(3), 528–547.

Lazarsfeld, P. (1957). Public opinion research and the classic tradition. *Public Opinion Quarterly, 21*, 39–53.

Lazarsfeld, P. F., Berelson, B., & Gaudet, H. (1944). *The people's choice. How the voter makes up his mind in a presidential campaign*. New York: Columbia University Press.

Lea, M., & Spears, R. (1995). Love at first byte? Building personal relationships over computer networks. In J. T. Wood & S. Duck (Eds.), *Under-studied relationships: Off the beaten track* (pp. 197–233). Thousand Oaks: Sage.

Lee, H. (2005). Behavioral strategies for dealing with flaming in an online forum. *The Sociological Quarterly, 46*(2), 385–403.

Leggewie, C. (2009). Die Medien der Demokratie. Eine realistische Theorie der Wechselwirkung von Demokratisierung und Medialisierung. In F. Marcinkowski & B. Pfetsch (Eds.), *Politik in der Mediendemokratie* (pp. 70–83). Wiesbaden: VS Verlag für Sozialwissenschaften.

Lembcke, O., Ritzi, C., & Schaal, G. (2012). Zwischen Konkurrenz und Konvergenz. Eine Einführung in die normative Demokratietheorie. In O. Lembcke, C. Ritzi, & G. Schaal (Eds.), *Zeitgenössische Demokratietheorie. Normative Demokratietheorien* (Vol. 1, pp. 9–32). Wiesbaden: VS Verlag für Sozialwissenschaften.

Lindner, R. (2007). *Politischer Wandel durch digitale Netzwerkkommunikation? Strategische Anwendung neuer Kommunikationstechnologien durch kanadische Parteien und Interessengruppen*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Lippmann, W. (1925). *The phantom public*. Piscataway: Transaction Publishers.

Liu, X., & Fahmy, S. (2011). Exploring the spiral of silence in the virtual world: Individuals' willingness to express personal opinions in online versus offline setting. *Journal of Media and Communication Studies, 3*(2), 45–57.

Maireder, A., & Schlögl, S. (2014). 24 hours of an #outcry. The networked publics of a socio-political debate. *European Journal of Communication, 29*(6), 687–702.

Matthes, J., Rios Morrison, K., & Schemer, C. (2010). A spiral of silence for some. Attitude certainty and the expression of political minority opinions. *Communication Research, 37*(6), 774–800.

McCoombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *The Public Opinion Quarterly, 36*(2), 176–187.

Meckel, M. (1999). Cyberpolitics und Cyberpolitik: Zur Virtualisierung politischer Kommunikation. In K. Kamps (Ed.), *Elektronische Demokratie? Perspektiven politischer Partizipation* (pp. 229–244). Wiesbaden: Westdeutscher Verlag.

Meraz, S., & Papacharissi, Z. (2013). Networked gatekeeping and networked framing on #Egypt. *The International Journal of Press/Politics, 18*(2), 138–166.

Messing, S., & Westwood, J. (2012). Selective exposure in the age of social media. Endorsements trump partisan source affiliation when selecting news online. *Communication Research*. https://doi.org/10.1177/0093650212466406.

Mouffe, C. (2000). *The democratic paradox*. London: Verso.

Moy, P., Domke, D., & Stamm, K. (2001). The spiral of silence and public opinion. On affirmative action. *Journalism and Mass Communication Quarterly, 78*(1), 7–25.

Muhlberger, P. (2003). Political values, political attitudes, and attitude polarization in Internet political discussion: Political transformation or politics as usual? *Communications, 28*(2), 107–133.

Muñiz, C., Alvídrez, S., & Téllez, N. (2015). European public sphere| Shaping the online public debate. The relationship between the news framing of the expropriation of YPF and readers' comments. *Journal of Communication, 9*, 3245–3263.

Mutz, D. C. (2006). Hearing the other side. In *Deliberative versus participatory democracy*. Cambridge: Cambridge University Press.

Negroponte, N. (1995). *Being digital*. New York: Vintage Books.

Neuberger, C. (2009). Internet, Journalismus und Öffentlichkeit. Analyse des Medienumbruchs. In C. Neuberger, C. Nuernbergk, & M. Rischke (Eds.), *Journalismus im Internet: Profession – Partizipation – Technisierung* (pp. 19–105). Wiesbaden: VS: Verlag für Sozialwissenschaften.

Neuberger, C. (2014). Konflikt, Konkurrenz und Kooperation: Interaktionsmodi in einer Theorie der dynamischen Netzwerköffentlichkeit. *Medien & Kommunikationswissenschaft, 62*(4), 567–587.
Nisbet, M. C., & Kotcher, J. E. (2009). A two-step flow of influence? Opinion-leader campaigns on climate change. *Science Communication, 30*(3), 328–354.
Nisbet, M. C., & Scheufele, D. A. (2004). Political talk as a catalyst for online citizenship. *Journalism and Mass Communication Quarterly, 81*(4), 877–896.
Noelle-Neumann, E. (1984). *Public opinion – Our social skin*. Chicago: University of Chicago Press.
Noelle-Neumann, E., Schulz, W., & Wilke, J. (Eds.). (2000). *Fischer Lexikon Publizistik Massenkommunikation* (7th ed.). Frankfurt am Main: Fischer Taschenbuch Verlag.
Nuernbergk, C. (2013). *Anschlusskommunikation in der Netzwerköffentlichkeit*. Baden-Baden: Nomos.
Nuernbergk, C. (2014). Follow-up communication in the blogosphere. *Digital Journalism*. https://doi.org/10.1080/21670811.2014.895520.
Papacharissi, Z. (2002). The virtual sphere. The Internet as a public sphere. *New Media & Society, 4*(1), 9–27. https://doi.org/10.1177/14614440222226244.
Papacharissi, Z. (2004). Democracy online. Civility, politeness, and the democratic potential of online political discussion groups. *New Media & Society, 6*(2), 259–283.
Papacharissi, Z. (2011). *A private sphere-democracy in a digital sphere*. Cambridge: Polity Press.
Pariser, E. (2011). *The filter bubble. What the Internet is hiding from you*. London: Viking.
Peters, B. (1993). *Die Integration moderner Gesellschaften*. Frankfurt a. M.: Suhrkamp.
Pfetsch, B., Adam, S., & Lance, B. W. (2013). The critical linkage between online and offline media. *Javnost – The Public, 20*(3), 9–22.
Porten-Cheé, P., & Eilders, C. (2015). Spiral of silence online. How online communication affects opinion climate perception and opinion expression regarding the climate change debate. *Studies in Communication Sciences, 15*(1), 143–150.
Price, V. (2008). The public and public opinion in political theories. In W. Donsbach & M. W. Traugott (Eds.), *The SAGE handbook of public opinion research* (pp. 11–24). London: Sage.
Putnam, R. D. (1995). Bowling alone: America's declining social capital. *Journal of Democracy, 6*(1), 65–78.
Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. New York: Simon & Schuster.
Reader, B. (2012). Free press vs. free speech? The rhetoric of "civility" in regard to anonymous online comments. *Journalism and Mass Communication Quarterly, 89*(3), 495–513.
Rheingold, H. (2000). *The virtual community. Homesteading on the electronic frontier*. Cambridge: MIT Press.
Rhomberg, M. (2008). *Agenda-Setting. Theorie der Mediendemokratie*. München: Willhelm C. Fink.
Rhomberg, M. (2009). *Politische Kommunikation. Eine Einführung für Politikwissenschaftler*. Paderborn: Fink/UTB.
Rhomberg, M. (2012). Public opinion. In G. Ritzer (Ed.), *The Wiley-Blackwell encyclopedia of globalization*. Boston: Blackwell.
Rogers, E. M. (2002). Diffusion of preventive innovation. *Addictive Behaviors, 27*, 989–993.
Rössler, P. (2008). Agenda-setting, framing and priming. In W. Donsbach & M. W. Traugott (Eds.), *The SAGE handbook of public opinion research* (pp. 205–217). London: Sage.
Rucht, D., Mundo, Y., & Zimmermann, A. (2008). *Politische Diskurse im Internet und in Zeitungen*. Wiesbaden: VS Verlag für Sozialwissenschaften.
Santana, A. D. (2011). Online readers' comments represent new opinion pipeline. *Newspaper Research Journal, 32*(3), 66–81.
Schäfer, M. S., & Taddicken, M. (2015). Opinion leadership revisited: A classical concept in a changing media environment. *International Journal of Communication, 9*, 960–981.
Scharpf, F. W. (1997). *Games real actors play*. Boulder: Westview.

Scheufele, D. A. (2008). Spiral of silence theory. In W. Donsbach & M. W. Traugott (Eds.), *The SAGE handbook of public opinion research* (pp. 175–191). London: Sage.
Schmidt, J.-H. (2013a). *Social media*. Wiesbaden: VS Verlag für Sozialwissenschaften.
Schmidt, V. A. (2013b). Democracy and legitimacy in the European Union revisited: Input, output and 'throughput'. *Political Studies, 61*(1), 2–22.
Schradie, J. (2011). The digital production gap: The digital divide and Web 2.0 collide. *Poetics, 39*(2), 145–168.
Schudson, M. (2008). The "Lippmann-Dewey debate" and the invention of Walter Lippmann as an anti-democrat 1985–1996. *International Journal of Communication, 2*, 1031–1042.
Schulz, W. (2011). Politische Kommunikation: theoretische Ansätze und Ergebnisse empirischer Forschung (3., überarb. Aufl. ed.). Wiesbaden: VS Verl. für Sozialwiss.
Schulz, A., & Roessler, P. (2012). The spiral of silence and the Internet. Selection of online content and the perception of the public opinion climate in computer-mediated communication environments. *International Journal of Public Opinion Research, 24*(3), 346–367.
Shoham, A., & Ruvio, A. (2008). Opinion leaders and followers. A replication and extension. *Psychology and Marketing, 25*(3), 280–297.
Sunstein, C. (2001). *Republic.com*. Princeton: Princeton University Press.
Sweetser, K. D., Golan, G. J., & Wanta, W. (2008). Intermedia agenda setting in television, advertising, and blogs during the 2004 election. *Mass Communication and Society, 11*(2), 197–216.
Takeshita, T. (2006). Current critical problems in agenda-setting research. *International Journal of Public Opinion Research, 18*(3), 275–296.
Tomaszeski, M., Proffitt, J. M., & McClung, S. (2009). Exploring the political blogosphere. Perceptions of political bloggers about their sphere. *Atlantic Journal of Communication, 17*(2), 72–87.
Trappel, J. (2011). Why democracy needs media monitoring. In J. Trappel, H. Nieminen, & L. Nord (Eds.), *The media for democracy monitor. A cross national study of leading news media* (pp. 11–28). Göteborg: Nordicom.
Trepte, S., & Scherer, H. (2010). Opinion leaders – Do they know more than others about their area of interest? *Communications, 35*(2), 119–140.
Turcotte, J., York, C., Irving, J., Scholl, R. M., & Pingree, R. J. (2015). News recommendations from social media opinion leaders. Effects on media trust and information seeking. *Journal of Computer-Mediated Communication, 20*(5), 520–535.
van der Merwe, R., & van Heerden, G. (2009). Finding and utilizing opinion leaders. Social networks and the power of relationships. *South African Journal of Business Management, 3*, 65–76.
van Dijk, J. (2006). Digital divide research, achievements and shortcomings. *Poetics, 34*(4–5), 221–235.
Wall, M. (2006). Blogging Gulf War II. *Journalism Studies, 7*(1), 111–126.
Warner, M. (2005). *Publics and counterpublics*. Cambridge: Zone Books.
Wimmer, J. (2007). *(Gegen-)Öffentlichkeit in der Mediengesellschaft. Analyse eines medialen Spannungsverhältnisses*. Wiesbaden: VS Verlag für Sozialwissenschaften.
Winsvold, M. (2007). Municipal websites in the local public debate. Supplying facts or setting agenda? *NORDICOM Review, 28*(2), 7–23.
Wojcieszak, M. E., & Mutz, D. C. (2009). Online groups and political discourse: Do online discussion spaces facilitate exposure to political disagreement? *Journal of Communication, 59*(1), 40–56.
Wolling, J., & Emmer, M. (2014). Individual political communication and participation. In C. Reinemann (Ed.), *Political communication* (pp. 449–468). Berlin/Boston: De Gruyter Mouton.
Woong Yun, G., & Park, S. (2011). Selective posting. Willingness to post a message online. *Journal of Computer-Mediated Communication, 16*(2), 201–227.
Zamith, R., & Lewis, S. C. (2014). From public spaces to public sphere. *Digital Journalism, 2*(4), 558–574.

Digitalization of Politics and Elections

23

Georg Hanschitz

Tech will transform from something we actively use to a more seamless integrated experience that is 'on' all the time
Daniel Bæk, Cofounder of Nodes, 2014

Contents

Abstract

This chapter is a contribution to the discussion on how cyber-development will transform present scopes of democratic participation into new online and multichannel-based structures of democratic partaking. In this context, the possibility of online voting is expected to be a significant instrument. Elections are the heartbeats of democracies, but it seems that the heartbeats of people nowadays follow their PEDs (Personal Electronic Devices) clock rate. Mobile technology is embedded in our lives and also in nearly all communication processes. Political

G. Hanschitz (✉)
Institute of Education and Innovation, Vienna, Austria
e-mail: mail@georghanschitz.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_3

campaign management and digital interactions via mobile applications have become more and more common in the political systems of the world. For years, project founders of new voting technologies have tried to implement people's interests in policy processes with the help of digital technologies. Since a new security technology of online financial services named block chain arrived in the global stock market and the US stock market Nasdaq launched the first trading platform on its base in 2015, it is time to discuss and adoption of this system in online voting (also called i-voting), making election processes more attractive and raise turnout.

Keywords
Cyber-development · Election · Block chain · Personal electronic devices · Online voting · Calculus of voting · Social media · Digital revolution of politics

Introduction: I-Voting, the Digital Revolution of Politics

Information and communication technologies (ICTs) changed the way of socio-political interaction all over the world. The digitalization of social interaction via mobile devices supported the globalization of personal and political life events, like political campaigns, elections or riots. Social platforms collect and produce social information from all over the world, in real-time. One can say that today's ICTs share and produce social information at the same time. Social media platforms are places of personal, social, political, and also knowledge interconnectivity. People all over the world are more and more used to interact and discuss on local- and global-level online. Structuring the predictable evolution-process from political online discussions to online decision-making could be a chance for democracies improving their quality of social interaction and may secure democratic partaking in a fast-growing digital sociality.

The use of Personal Electronic Devices (PED) and telecommunication devices rises every year worldwide and the things we do and how we run our lives are more and more connected with these PEDs. Home is where Wi-Fi is – Wireless Fidelity seems to be what today's world is all about. Everywhere around us we notice someone using a mobile device like a smart phone, tablet, or smart watch. Today, being mobile allows us to use digital services that we rely on. We love our PEDs. We stay informed via PEDs, we check our mails, our body fitness, we train our brain, and we share potential romantic issues on dating apps. Uber, Facebook, Tinder, and Twitter changed the way we see the world today, because these services make us feel that every social interaction is possible, shareable, and steerable in the second we write, like, and share. The digital media consumption on mobile devices in the USA from 12/2010 to 12/2014 shows that "mobile has moved from being a way to consume content to a platform that helps us accomplish more all day, every day. Smartphone usage is up 394 percent, and tablet usage is up a whopping 1,721 percent as these platforms now combine to account for 60 percent of digital media time spent" (Dreyer 2015). Having these stats in mind and taking into account that numbers of political events between 2010 and 2014 were highly connected to the usage of mobile devices, it is highly verifiable that mobile devices and social

networks not only changed our daily life but also our way of political interaction. Revolts and protests connected with high usage of the social networking site Twitter by protestors and demonstrators that shaped the term "Twitter Revolution" (PEJ New Media Index 2009) over the past 5 years.

Examples of social network forced events with high international response by journalists and politicians had been the 2009 Moldova civil unrest, the Iranian election protest (Green Revolution, Facebook Revolution), the Tunisian revolution 2011, also known as Jasmine Revolution or Wikileaks Revolution, the Egyptian Revolution of 2011, and the Euromaidan Revolution in Ukraine, beginning in November 2013 (Buettner 2015). The way we consume information and content changed significantly. Since 2014, the majority of "Digital Media Consumption" takes place in "Mobile Apps" in the USA. US digital media users are spending the majority of their time-consuming digital media within mobile applications, according to a study released by comScore, 2014 (Perez 2014). So when we take into account that these users also consume political information and policy issues via their PEDs, then we have to ask probably why government do not give them the right to politically interact and vote via their PEDs. Electronic voting has been a huge issue during the last 10 years but the increase of PED communication could be a game-changer in the e-voting discussion. Using electronic tools to record and count votes today is implemented via different Internet services and devices from touch screen voting machines and kiosks (Direct Recording Electronic Voting Machine) located at polling stations to i-voting software (Public Direct Recording Electronic Voting) where people vote at home without going to a polling station.

Integration of Online Voting in the Election Process and Security Issues

Today, every daily task can be done mobile via Internet, but why cannot we vote online? While in some states the system of DRE kiosks are still discussed and also provide not 100% security and valid results (e.g., Florida Congressional Elections: November 2006 – in Lin and Espinoza (2007)), other states changed to i-voting using the public network for their voting system like Estonia. Today, a lot of countries use or test i-voting in municipal elections, like Canada, Sweden, Latvia, and Switzerland, but Estonia uses an i-voting system for the national elections. The Estonian system allows voters to "cast their ballots from any Internet-connected computer, anywhere in the world." *"Unrelated to the electronic voting systems used elsewhere, which involve costly and problematic machinery, the Estonian solution is simple, elegant and secure. During a designated pre-voting period, the voter logs onto the system using an ID card or Mobile ID, and casts a ballot. The voter's identity is removed from the ballot before it reaches the National Electoral Commission for counting, thereby ensuring anonymity. With any method of remote voting, including traditional mail-in ballots, the possibility of votes being forced or bought is a concern. Estonia's solution was to allow voters to log on and vote as many times as they want during the pre-voting period. Since each vote cancels the last, a voter always has the option of changing his*

or her vote later. In 2005, Estonia became the first country in the world to hold nation-wide elections using this method, and in 2007, it made headlines as the first country to use i-voting in parliamentary elections. Thanks to its convenience, i-voting is proving highly popular with the Estonian electorate. In the European Parliament elections 2014, 31,3 percent of voters cast their ballots in this way. In the case of i-voting, the cumulative time savings in the Estonian parliamentary elections of 2011 were 11,000 working days, which would amount to around 504,000 Euros in average wages. In the 2015 Parliamentary Elections, Internet voting accounted for 30,5 percent of the votes cast. Estonians worldwide cast their votes from 116 different countries," (Estonia Government Homepage 2016). Estonia's National Electoral Committee spokesman Priit Vinkel told *CNN* in 2011 that the Estonian Internet voting relies basically on a single factor: "trust." But how secure is i-voting? "In Estonia, that security includes a national ID card that can be used remotely and a voting system built to recognize unusual activity, Vrinkel said. He said security officials have detected no serious attempts to tamper with the votes" (Gross 2011). But still there are questions like could the "internet's known security risks alone be enough to call an election's results into question" – Avi Rubin, a professor of computer science at Johns Hopkins University who specializes in computer security says confronted by the results of the Estonian election system. "People's computers are not getting more secure, Rubin said to CNN. They're getting more under the control of malware" (Gross 2011). This may be true and nevertheless trillions of Euros and Dollars are right now moving around the world via online banking and also sensitive data like tax-data and social security numbers are available online, like in Austria where one is able to edit high sensitive personal data via www.finanzonline.at (Austria Government 2016).

Speaking about Austria, the presidential elections in 2016 demonstrate that security issues are not limited to digital systems only.

The first round of presidential elections in Austria were held on April 24th 2016 without any reported problems. The second round, a run-off on 22 May 2016, was declared invalid by the Constitutional Court on July 1st. Reason: Postal ballots were processed before the official start of the count on the morning after the election. Counts also were carried out in absence of party observers, the Court noted. The election was rescheduled on October 2nd but then 3 weeks before, the date delayed to 4th of December 2016 because of defective envelopes. The glue on postal vote envelopes has become unstuck in a significant number of cases. Based on these events, the leader of the Austrian Peoples Party and Vice-Chancellor Reinhold Mitterlehner stated in an interview with the public service radio station Ö1 on September 14th 2016 that he would appreciate the implementation of E-Voting in future elections, also with a reference to the Estonian system (Mitterlehner 2016).

The Block Chain Security System

The answer of security questions concerning i-voting could be given by a simple but effective system that stands behind the worldwide most popular peer-to-peer electronic cash system – Bitcoin. Bitcoin could be the i-Voting Game Changer:

Bitcoin is a "purely peer-to-peer version of electronic cash" which allows online payments to be sent "directly from one party to another without going through a financial institution" without double-spending (Nakamoto 2009). The security system behind Bitcoin is very simple: "The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work" – the block chain. The block chain is the key behind the security system: "The block chain is a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending Bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography" (Nakamoto 2009). This means that the whole network documents proves and secures all transactions by writing them down and connect them without any possibility to change any data without alarming the whole network.

For years, i-voting had been discussed under the aspect of security and insecurity of the World Wide Web, it seems that the block chain technology has the ability to become a new standard of verified processes in the Internet. The huge advantage of this system is that the block chain is not manipulable by computer viruses or any other kind of device-based malware, because all the data is secured by all participants of the global network and every move or transaction is noticed. For users, it is therefore possible to prove the ownership of rights or goods of a specific participant at all time.

For better understanding, two examples guide through the process – the first is a business transaction and the second is a possible election process via i-voting.

Block Chain Model, A Buys from B

1. The Deal: Person A buys from person B.
2. Verification: Now the block chain comes into play, a database that acts as a registry for money units. About the block chain, the buyer can identify the unit among thousands other explicitly and realize that the seller is actually the rightful owner of the unit. He can be sure not to buy fake units (or stolen goods).
3. The Transaction: The information about the new owner of the unit is turned into a block of data. The information is encrypted; bystanders cannot recognize who is involved in the transaction. Anonymity is another advantage of the chain block.
4. Validation: The block chain exists in copy on many computers, which are interconnected via the Internet. They all check the data block, and the transaction. If someone falsifies the information of a unit, it is recorded by the whole network, and the transaction will be ignored. The decentralized nature makes manipulation difficult.
5. Implementation: Is the transaction verified, it will be added to the block chain. Because the block chain cannot be changed but only complemented, the whole transaction is traceable in the future – just like any other recent transaction.

6. The result: The block chain reports person A now as owner of the unit. Person B therefore cannot sell it a second time, even if the unit itself is still in his possession.

The level of this decentralized security system is so high that leading bank institutes have problems to argue their international proved money system. Not only the so-called Fintechs but also established bank institutes trust the block chain system; today, dozens of banks try to implement the technical standard of bock chains, even the German Bank and Commerzbank. In 2015, the US stock market Nasdaq launched the first trading platform on block chain base (Hope and Casey 2015). The exact same procedure can be used to verify a vote in an election process.

Block Chain Model, A is Voting B

1. The Election: Person A is voting person B via a mobile device or desktop computer.
2. Verification: The block chain registers the voting decision and identifies the voter whether he or she has actually the right to vote via an encrypted governmental register.
3. The Transaction: The information about the decision is turned into a block of encrypted data. Observers do not recognize who is involved in the decision – not the identity of the person who votes nor the candidate can be made out.
4. Validation: The computers in the network check the data block. No one is able to manipulate the decision and or any information from outside. All data is encrypted and recorded by the whole network. Any manipulation will be ignored.
5. Implementation: If the process verified, it will be added to the block chain and linked with all other decisions made in the election so far and later on. The block chain can only be complemented by other verified decisions.
6. The result: The block chain reports to person A that person A now voted and the vote is verified. The whole election and every single decision are traceable for governmental officers without seeing people's names. Only the single voter has the possibility to trace his or her decision plus place and time of sending.

In late 2015 and 2016, various online platforms started to implement the block chain in election processes. One of the most known platforms is http://www.bitcongress.org – BitCongress is a platform that can be used by "states, schools, churches, businesses, individuals or groups of any kind" for "Law Creation, Voting, Debate, Community Budgeting, Decision Making." The platform allows designing a question or a whole election and uses so called "Vote-Tokens" which can be generated for each voter. All votes are registered by the block chain and can be comprehended a hundred percent. Giving a vote is possible via Internet or a mobile application, called AXIOMITY.

Other platforms like https://followmyvote.com calls to join the "Parallel Presidential Election of 2016" or the http://www.v-initiative.org say that they "distribute

100% fraud proof 100% anonymous digital votes." In reality, they just adopt the secure and simple Bitcoin technology and design voting-apps – something governments could simply do by their own (Daniel 2015). But why should they do that? The answer of this question is the hypothesis of this chapter. I-voting can raise voter turnouts and make democracy more democratic again.

The voter turnout is the percentage of eligible voters who actually go and vote. For many years, in most established democracies, there has been a trend of decreasing voter turnouts. A low turnout is undesirable, because than the vote that counts is not the comparative representation of the people in the country (able to vote) but maybe the representation of a minority of people who actually go to the polls. Research of "economic, demographic, cultural, technological, and institutional factors" is made to increase turnout and encourage voting. In the US 2012 presidential election, the turnout was 55%, and in the European Union Parliament Elections in 2014, the turnout was 42.61%.

The Rational Choice of Voting

The basic calculus of voting is based on rational choice theory, which says that social behavior results from individual actors and their individual decisions. The theory focuses on individual choices based on available choice alternatives and preferred options (Downs 1957). In the calculus of voting, the individual's effect on the election (P) and the assumed (personal) positive benefit (B) are both combined and aggregated with the social/personal gratification of voting and being part of the voter-community (D) and set in proportion with the time and financial effort (ex. to get to the polls) of the voting process (C). The original formula is $PB + D > C$, people vote when the assumed individual effects on the result and the perceived benefit plus social/personal gratification together, have to be bigger than the time financial efforts involved in voting (Riker and Ordeshook 1968).

To test how P and B influence turnouts, two professors Ryan D. Enos (Harvard University) and Anthony Fowler (University of Chicago) made a field experiment in the aftermath of a tied election and published the results in 2014 – in an article called "Pivotality and Turnout: Evidence from a Field" (Enos and Fowler 2014). The background: "The 2010 November election for Massachusetts State House in the 6th Worcester District ended in a dead heat. After a series of recounts and a court case, Geraldo Alicea, the Democratic candidate, and Peter Durant, the Republican candidate, had each received exactly 6587 votes. A special election was scheduled for 10 May 2011, and the race was likely to be close again. The same candidates who had just produced the tie would square off again with the same voters." To show evidence and generate data, Enos and Fowler placed phone calls to registered voters "to remind them about the special election and inform a random subset about the exact tie in the previous election." The result of the field experiment they found only "little evidence that the closeness of elections and considerations of pivotality motivate voters to turn out." Another factor which has to be taken into account discussing pivotality is the discrepancy of P being smaller in elections with higher

turnouts, resulting that PB is smaller too. B is the evident benefit of the voted political party or candidate – PB sets B in relation to the single vote P. But B does not necessarily only include personal interests but also social welfare, party interests, and interests of majorities or minorities in the society (Fowler 2006). If Voters think that others also benefit from the outcome of their choice, they have to be interested not only on their act of voting but the sum of voting decisions, which lead us to D, the voting culture. In 1968, Riker and Ordeshook developed "five major forms of gratification that people receive for voting: complying with the social obligation to vote; affirming one's allegiance to the political system; affirming a partisan preference; affirming one's importance to the political system; and, for those who find politics interesting and entertaining, researching and making a decision" (Riker and Ordeshook 1968). Back to the hypothesis of i-voting may have positive effect on turnouts, (social) PED applications could strengthen the social gratification people receive for voting. This could lead to a double effect: Factor C, the time investment and financial effort of the voting process or getting to the polls could be set down to nearly zero – at least for PED users via voting-apps (mobile device voting applications). At the same time, the social factor D could be strengthened by voluntarily sharing the act of voting and maybe also personal reasons and assumed positive effects through an integration of voting-apps in social networks. In countries with voter registration processes like the USA, both steps – registration and voting could be made via PEDs in future. In two-step systems, the double effect of ease of voting and social gratification via PEDs could take place both times, in the registration process and in the elections.

In some areas in the world, polling centers are hardly accessible and elections take days. At the same time, mobile or satellite network are accessible easily and i-voting could be a true democratic factor. One has to state that in low-developed countries, an i-voting system via PEDs would be a huge financial factor for governments. In these states, special voting PEDs and DREs (Direct Recording Electronic) like mobile voting machines would be need. But for the voters themselves, the factor of cost and time could be reduced tremendously.

Social Media and the Calculus of Voting

Back to the European Union, "the turnout for the European elections fell by almost 19 points between 1979 and 2009, from 61.99% to 42.54%" although European Parliament has conducted "a large-scale attempt to boost turnout in the 2014 elections, investing in a social media campaign" (EurActiv.com 2014). The difficulty of political social media campaigning in correlation with turnout is to overcome the gap between a well-designed online marketing campaign and the paper-based voting process. People in the European Union are used to get information via PEDs, but there is no culture of bringing their PEDs to the polls to scroll down information and names during the voting process. This is a cross-media gap which cannot be solved by online marketing. It is more likely that voters bring business cards of their favorite candidates to the polls to be sure of writing candidate names and numbers

correctly, than to switch on their smart phones. In 2012, CNN and Facebook presented the "I'm Voting App" (https://apps.facebook.com/cnnimvoting, accessed 2/2016) where "385,096 people have pledged to vote in the 2012 U.S. Election" (https://www.facebook.com/cnn?sk=app_195983790531602&iid=article_sidebar, accessed 2/2016). The app was created by the marketing agency Tenthwave (http://www.tenthwave.com, accessed 2/2016) and enabled Facebook users to "commit to vote for and endorse specific candidates and issues, and their commitments will be displayed on their timelines, news feeds, and tickers" and was available for desktop computers and mobile devices. The affect on the turnouts had not been measured but the turnout of the 2012 presidential election, which was named "to be most social in history" (Cohen 2012), had been 54.9% which is lower than 2008 (57.1%) and 2004 (55.7%). Also in this case, like in the EU elections of 2014, the gap between social media involvement, the implementation to the voting process, and the turnout could have played a role.

The C-Factor and the Limitation of Possibilities

One hurdle of high turnout is still factor C – the obstacles to get to the polls. In a lot of countries like France, Germany, and Austria, elections are on Sundays to lower the time and cost investment of workers and employees, but at the same time, campaign managers of all parties hope for certain weather conditions which may affect the turnouts (Eisinga et al. 2012). In 2014, a study of the University of Gothenburg, Department of Political Science showed that in Sweden, rainfalls during the Election Day have no negative effects on the turnout (Perssona et al. 2014). In the USA, "the relationship between bad weather and lower levels of voter turnout is widely espoused by media, political practitioners" and a study on "the effect of weather on voter turnout in 14 U.S. presidential elections using meteorological data drawn from over 22,000 U.S. weather stations to provide election day estimates of rain and snow for each U.S. county" showed that when "compared to normal conditions, rain significantly reduces voter participation by a rate of just less than 1% per inch, while an inch of snowfall decreases the turnout by almost .5%." In the study, "poor weather is also shown to benefit the Republican Party's vote share." "Indeed, the weather may have contributed to two Electoral College outcomes, the 1960 and 2000 presidential elections," the study says (Gomez et al. 2007). To lower the C-factor connected with any weather conditions, i-voting could be a sustain instrument which may be also able to overcome the gap between our daily PED interaction, social network communication, and the aim of democracies reaching close involvement of citizens and high turnouts. The factor time is not only an issue during the Election Day but also a huge factor when it comes to the voter's decision, which can be made days or hours before.

Politicians and campaign managers try nearly everything to influence the voter's decision-making process. One possible decision formula in campaigning could be "look, inform, think, decide" and another could be "look, inform, feel, decide" – TV-spots, public debates, newspaper, and media marketing do their best to

transport image and content of political parties and candidates. At the end, the decision-making process can be interfered through information overload (Yang et al. 2003). To ease the decision-making process on the Election Day, PED involvement and a simple reminder of the decision day including names and profile pictures of candidates can help to focus on the decision-making process and positively affect the turnouts.

Online dating apps like "Tinder" or "Hot or Not" use simplification to find possible partners. There are billions of people and billions possible partners in the world – impossible to inform, think, decide – so the user gets pictures and simple information about candidates and then can decide whether yes or no. The decision-making process is simplified from billions of possibilities to yes or no. In this field, the C-factor of decision making went from infinite to limited. The same technique could be used in voting-apps – after weeks of campaigning, the voter could be enabled able to scroll down the candidates and simplify the decision to a single or serial yes and no answers – a limitation of factor C.

The D-Factor, Social Duty, and Behavioral Nudging

In the "Economic Theory of Democracy" of Anthony Downs, 1957, presents the factor D as social duty (Downs 1957), and in a lot of countries, there had been an obligation to vote. In 2013 compulsory voting was still used in 22 countries (11 of these 22 countries enforce these laws in practice) according to the Central Intelligence Agencies "World Factbook" 2013 (CIA 2013). In other countries, a new system was applied which Riker and Ordeshook referred to in "A Theory of the Calculus of Voting" in 1968 where positive civic benefit and behavior and psychological goodwill feeling would strengthen the choice to vote. Social factors are playing a huge role when it comes to the voting process. A lot of people used to meet neighbors and friends an Election Day, especially in rural regions. Today, in many countries, postal voters become more and more relevant and "vote-by-mail elections" common – and in the USA, in 2008, "drive-thru voting" was allowed in some areas. In California's El Dorado and Sonoma counties and Douglas County, Oregon voters could leave their "absentee ballots in a drop-box at designated locations" (drop-offs 24/7). El Dorado County officials said to the *Wired* magazine in 2008 that "more than 500 people have taken advantage of the box and saved a bit of change on their postage" (Squatriglia 2008). The idea behind projects like the drive-thru-voting is still to lower the C-factor of the Calculus of Voting, but the result is a lower D factor also, because social interaction is near to zero in a drive-thru process.

To strengthen the D factor, it may need a little nudge ("nudge," "a light touch or push," definition Oxford English Dictionary, 2016): In 2008, the "nudge theory" became popular around the world very soon. Cass Sunstein, founder and director of the Program on Behavioral Economics and Public Policy at Harvard Law School and former Administrator of the White House Office of Information and Regulatory Affairs, and coauthor Richard H. Thaler started a hype with their book "Nudge: Improving

Decisions about Health, Wealth, and Happiness" (Sunstein and Thaler 2008), followed by "Simpler: The Future of Government (2013) and most recently Why Nudge? (2014)." The concept behind the nudge theory is the hypothesis that behavior can be influenced "in a predictable way without forbidding any options or significantly changing economic incentives," it is directing people to make good choices "without restricting" the "freedom of choice" (Sunstein and Thaler Q/A, n.d.). In our case talking about elections and the turnouts, the good decision would be to decide to vote. But here the concept of nudging may lead to a dead end – there is a high chance that people know that elections are important for their democratic system and they potentially would answer yes if asked whether elections are important for their lives or not. Nevertheless, there are high percentages of nonvoters in a huge number of elections because the choice of candidates leaves them puzzled. Governments can install road signs on election day to nudge people to go to the polls, political parties can make phone calls to bring people to the voting machines, but at the end, the decision maker has to decide whether to go to the polls or not – and whom to vote. Taken this into account, stigmatization of nonvoters does not work. Voters should have a strong incentive to show that they are engaged in the election process. They should be able to feel informed about the political affairs at stake, the whole election process and see themselves as social capital, nudging others to vote too.

Social networks have changed the nightlife of people – with every disclosed guestbook of an event, the question arises if it would not be a shame not to go there, taken into account that nearly all friends are going (or seem to). After the event, hundreds of pictures will remind both participants and nonparticipants about the big night and what nonparticipants missed out.

This kind of social publicness could be used for elections too – one of the applications in this field had been the "I'm Voting App" mentioned before, but giving people the chance to vote via their PEDs and sending their decision to vote directly to all other friends in all social networks they are in would lead to a potentization of the public event effect – a massive strengthening of the D factor could be result.

Critical Aspects

The use of Personal Electronic Devices (PED) in social communication led to a phenomenon called "instagram narcissism" (Sheldon 2016) which is the description of a social behavior-making self-pictures (selfies) while doing things at all time – from starting in the day, eating to the seconds before falling asleep. In a digital social culture of instagram, narcissism secret voting is more and more at danger. People make selfies of their ballots and publish them in public social networks. I-voting could be a tool to push this phenomenon to another critical level, altering the positive effects of social interaction into negative.

Talking about security issues, the discussion about block chain technology in elections has gone quite far nowadays and it seems to be clear that this technology could be a real solution on the danger of manipulation from outside but still would be

possible to steal someone's PED to vote in his or her name with enough personal data knowledge. Right now, fingerprint technology came across the mobile phone market, but there is evidence that also this technology can be manipulated (Flynn 2014, Huffington Post).

Another critical aspect could be the gap between PED users, or digital natives, and non-PED users. There are generations of people who are convinced that digital processes are unsafe. Some of them do not use PEDs at all, and some use only for telecommunication. A high percentage of i-voters could lead to closing of numbers of polling stations. The nondigital election infrastructure could erode artificially.

The most important critical aspect of the presented concept of i-voting is that no government has adopted and built such a system until now. This means that if a country or state decides to apply such a voting system, the electoral officials have to buy company-owned technology or (even more risky mandate) contract one of the service companies to execute the election via their system. In such an example, electoral officials have to be highly trained by IT-experts and have to get full access to all data in the data room of the contracted service company. It would be nearly impossible for outside election observers (like OSCE election observers) to "observe the entire electoral process" (OSCE 2016).

Conclusion

Being mobile allows us to use digital services wherever we are physically. Social network forced events are becoming more and more important and the consummation of information via PEDs lead to the wish of digital political interaction. Electronic voting has been a huge issue during the last 10 years but had been called unsafe. Now, new technologies allow high-security transfers and other aspects of i-voting get in front, like the advantage of social nudging via public social networks.

The basic calculus of voting has two important variables, the social/personal gratification of voting and being part of the voter-community (D) and the time and financial effort people have to make to be part of the voting process (C). I-voting may have positive effects on turnouts: Factor C, the time investment and financial effort for voters is nearly zero and at the same time, the social factor D could be strengthened by voluntarily sharing fact that someone just voted (and why). Politicians and campaign managers try nearly everything to influence the voter's decision-making process which can lead to an information overload. To ease the decision-making process on the election day, PED involvement and a simple reminder could can help to focus on the decision-making process and the election itself. More than that, i-voting has the possibility to make the voting process more social again by giving people the chance to share their experience with friends in social networks.

It is foreseeable that there will be a spill over of i-voting from simple business applications like marketing surveys to complex social applications like municipal and federal elections. The challenge will be to implement an independent i-voting system which can be observed by officials without any kind of offering unnecessary personal information or other kind of sensitive data.

Referring to the concept of cyber-democracy, where free online communication, information, and interaction promote democracy as a whole, present scopes of democratic participation will soon transform into multichannel-based structures of democratic partaking.

Transferring elections via apps to peoples PEDs like smart phones, tablets, and smart watches will not only change the way of voting but also the possibility voters have to discuss and rethink decisions. It will influence the whole political communication in election campaigns – the goal in future campaigns will be to link with voters much more personal and until the very last second of their decision-making process.

PED applications will have to ask voters about their personal needs, hopes, and challenges and send unfiltered feedback to campaign war rooms, journalists, and social media platforms until the moment of decision. With all advantages and challenges for democratic societies, the today's secret personal voting decision may soon be part of a transparent, global, social media event.

References

Austria Government, Financial Service. (2016). https://finanzonline.bmf.gv.at/fon. Accessed 4 Feb 2016.

Bæk, D. (2014). Past, present and future of mobile apps: Interview with Daniel, managing partner of Nodes. http://www.nodesagency.com/present-and-future-of-mobile-apps-interview-with-daniel-managing-partner-of-nodes. Accessed 7 Jan 2016.

Buettner, R. (2015). A systematic literature review of Twitter research from a socio-political revolution perspective. https://doi.org/10.13140/RG.2.1.4239.9442.

CIA, Central Intelligence Agency. (2013). World factbook: Suffrage at Central Intelligence Agency. Retrieved 16 Aug 2013. https://www.cia.gov/library/publications/the-world-factbook/geos/eg.html. Accessed 1 Jan 2016.

Cohen, D. (2012). Facebook, CNN launch I'm Voting App. http://www.adweek.com/socialtimes/facebook-cnn-launch-im-voting-app/401184. Accessed 1 Feb 2016.

Daniel, M. (2015). Blockchain technology: The key to secure online voting, bitcoinmagazine. https://bitcoinmagazine.com/articles/blockchain-technology-key-secure-online-voting-1435443899. Accessed 1 Feb 2016.

Downs, A. (1957). Economic theory of democracy. New York: Harper & Row, *Journal of Political Economy*, *65*(2), 135–150. Published by University of Chicago Press. Stable URL: http://www.jstor.org/stable/1827369. Accessed 2 Feb 2016.

Dreyer, K. (2015). Mobile Internet usage skyrockets in past 4 years to overtake desktop as most used digital platform, Digital Future in Focus report. https://www.comscore.com/Insights/Blog/Mobile-Internet-Usage-Skyrockets-in-Past-4-Years-to-Overtake-Desktop-as-Most-Used-Digital-Platform. Accessed 3 Feb 2016.

Eisinga, R., Grotenhuis, M., & Pelzer, B. (2012). Weather conditions and voter turnout in Dutch national parliament elections, 1971–2010. Springer. https://doi.org/10.1007/s00484–011–0477-7. Accessed 3 Feb 2016.

Enos, R. D., & Fowler, A. (2014). Pivotality and turnout: Evidence from a field experiment in the aftermath of a tied election. *Political Science Research and Methods, 2*, 309–319. https://doi.org/10.1017/psrm.2014.5. http://journals.cambridge.org/abstract_S2049847014000053. Accessed 4 Feb 2016.

Estonia Government Homepage. (2016). https://valitsus.ee/en. Accessed 4 Feb 2016.

EurActiv.com. (2014). Efficacité et Transparence des Acteurs Européens, PLC. http://www.euractiv.com/sections/eu-elections-2014/its-official-last-eu-election-had-lowest-ever-turnout-307773. Accessed 2 Feb 2016.

Flynn, K. (2014). Your iPhone can be hacked with a photo of your thumb, Huffington Post, 12/31/2014, Content: "Jan Krissler, a German hacker demonstrated the hack at the annual Chaos Computer Club convention on Dec. 27. 2014" published on http://www.huffingtonpost.com/2014/12/30/hack-phone-fingerprint-photographs_n_6395730.html. Accessed 4 Feb 2016.

Fowler, J. H. (2006). Altruism and turnout. *Journal of Politics*, *68*(3), 674–683. University of California, August 2006. fowler.ucsd.edu/altruism_and_turnout.pdf. Accessed 3 Feb 2016.

Gomez, B. T., Hansford, T. G., & Krause, G. A. (2007). The republicans should pray for rain: Weather, turnout, and voting in U.S. presidential elections, 2007, published in the *Journal of Politics*. http://myweb.fsu.edu/bgomez/GomezHansfordKrause_JOP_2007.pdf. Accessed 17 Oct 2015.

Gross, D. (2011). CNN, Why can't Americans vote online? Updated 1609 GMT (0009 HKT) November 8, 2011. http://edition.cnn.com/2011/11/08/tech/web/online-voting/index.html. Accessed 4 Feb 2016.

Hope, B., & Casey, M. J. (2015). A bitcoin technology gets Nasdaq Test, pilot to take place in fledgling Nasdaq Private Market. http://www.wsj.com/article_email/a-bitcoin-technology-gets-nasdaq-test-1431296886-lMyQjAxMTE1MzEyMDQxNzAwW. Accessed 4 Feb 2016.

Lin, G., & Espinoza, N. (2007). Florida congressional elections: November 2006, Stanford University, United States, 2006. http://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/electronic-voting/index_files/page0004.html. Accessed 4 Feb 2016.

Mitterlehner, R. (2016). (ITV) in Ö1 Morgenjournal 14th September 2016, audio reference: http://oe1.orf.at/programm/448228

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. www.bitcoin.org. Accessed 4 Feb 2016.

Nudge. (2016). Definition: "A light touch or push." The Oxford Pocket Dictionary of Current English. 2009. Encyclopedia.com. Accessed 4 Feb 2016.

Online Index, PEJ New Media Index. (2009). Iran and the Twitter revolution, PEJ, New Media Index June 15–19, 2009, Pew Research Center 1615 L street, NW, Suite 800 Washington, DC 20036. http://www.journalism.org/2009/06/25/iran-and-twitter-revolution. Accessed 4 Dec 2015.

OSCE. (2016). Election observers, information. http://www.osce.org/employment/43290. Accessed 4 Feb 2016.

Perez, S. (2014). Majority of digital media consumption now takes place in mobile apps. http://techcrunch.com/2014/08/21/majority-of-digital-media-consumption-now-takes-place-in-mobile-apps, accessed 24 Nov 2015, referring to the U.S. Mobile App Report, August 21, 2014, http://www.comscore.com/Insights/Presentations-and-Whitepapers/2014/The-US-Mobile-App-Report. Accessed 4 Feb 2016.

Perssona, M., Sundella, A., & Öhrvallb, R. (2014). Does election day weather affect voter turnout? Evidence from Swedish elections. *Electoral Studies*, *33*, 335–342. http://www.sciencedirect.com/science/article/pii/S0261379413001212. Accessed 1 Feb 2016.

Riker, W. H., & Ordeshook, P. C. (1968). A theory of the calculus of voting. *American Political Science Review*, *62*. www.uky.edu/~clthyn2/PS671/Riker_1968APSR.pdf. Accessed 4 Feb 2016.

Sheldon, B. (2016). Instagram: Motives for its use and relationship to narcissism and contextual age. *Computers in Human Behavior, 58*, 89–97. https://doi.org/10.1016/j.chb.2015.12.059.

Squatriglia, C. (2008, November 4). It's time for drive-thru voting. Wired Magazine. http://www.wired.com/2008/11/it-is-time-for. Accessed 19 Jan 2016.

Sunstein, C. R., & Thaler, R. H. (2008). Nudge: Improving decisions about health, wealth, and happiness. e-book online https://ethicslab.georgetown.edu/studio/wordpress/wp-content/uploads/2015/02/Richard_H._Thaler_Cass_R._Sunstein_Nudge_Impro_BookFi.org_.pdf. Accessed 4 Feb 2016. Cass R. Sunstein biography data taken from http://hls.harvard.edu/faculty/directory/10871/Sunstein. Accessed 4 Feb 2016.

Sunstein, C. R., & Thaler, R. H. (Q/A, n.d.). Questions for Richard Thaler and Cass Sunstein http://www.amazon.de/Nudge-Improving-Decisions-Health-Happiness/dp/0141040017. Accessed 4 Feb 2016.

Yang, C., Chen, H., & Honga, K. (2003). Visualization of large category map for Internet brows. *Decision Support Systems, 35*, 89–102. https://doi.org/10.1016/S0167-9236(02)00101-X.

Knowledge Society, Knowledge Economy, and Knowledge Democracy

24

Nico Stehr and Alexander Ruser

Contents

Abstract

Knowledge has become the vital economic resource, especially as the basis of economic growth; but knowledge also is force in other social institutions of modern society, including of course, in governance or the world of work. It also is the case that certified scientific and technical knowledge claims have become the source of many of the social, political and personal problems confronting the economy, the state and the communities of modern societies

Our contribution is based on numerous publications surrounding the theoretical concept of the knowledge society and the phenomenon of knowledge, beginning in 1984 (see Böhme and Stehr 1984). A number but not all relevant publications are listed in the bibliography (for a recent discussion of the concept of the knowledge society see Stehr 2016).

N. Stehr (✉)
Karl Mannheim Chair of Cultural Studies, Zeppelin University, Friedrichshafen, Lake Constance, Germany
e-mail: nico.stehr@t-online.de

A. Ruser
Zeppelin University, Friedrichshafen, Germany
e-mail: Alexander.ruser@zu.de

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_16

worldwide. After all it was science and technology that discovered key global challenges of the modern age like ozone depletion, climate change, genetic engineering and the profound transformation of work. What will the future of knowledge societies look like?

Keywords
Knowledge · Information · Knowledge society · Economy · Democracy · Cyber-democracy · Fragility of social life

Earlier *theories of soc*iety choose to designate, quite properly, those attributes of social relations constitutive of the specific nature and era of that society as their identifying labels. Thus, such names as "capitalist" society or "industrial" society were created. For the same reasons, the now emerging form of society represents a "knowledge" society because the constitutive mechanism or the identity of modern society increasingly is driven by "knowledge." And as one of the early theorist of the knowledge society, Robert Lane (1966: 653) summarizes his definition of the "Knowledgeable Society: "The knowledgeable society is characterized by a relative emphasis upon certain ways of thinking, a certain epistemology, or, at the very least, a certain *knowledge about knowledge* (our emphasis)."

We would like to characterize knowledge not as something *that is so* which is a parochial conception of knowing but as a generalized capability to act on the world, as a model for reality, or as the ability to set something in motion (Stehr 1994). Knowledge represents *a capacity to act*. If defined in such a broad sense and therefore not restricted to scientific knowledge, we can designate, following Georg Simmel (1906: 441), e.g., knowledge as an anthropological constant: "All relationships of people to each other rest, as a matter of course, upon the precondition that they know something about each other." Similarly, power has been frequently based on advantages in knowledge, not only on physical strength. Societal reproduction is not merely physical reproduction but, in the case of humans, always cultural, i.e., reproduction of knowledge. Moreover, knowledge in the general sense as employed here is not restricted to any particular social system in modern societies. Knowledge is everywhere (see Luhmann 1990: 147).

Specifically, Knowledge has become the *vital* economic resource, especially as the basis of economic growth (Drucker [1968] 1972: 40; Böhme and Stehr 1986; Stehr 2002; David and Foray 2003); but knowledge also is force in other social institutions of modern society, including of course, in governance. It also is the case that certified knowledge claims especially scientific knowledge has become the source of many of the problems confronting modern societies. After all it was science that discovered key global challenges like ozone depletion, climate change or genetic engineering (cf. Stehr 2005; Grundmann and Stehr 2012; Oreskes and Conway 2011).

In retrospect, one is able to describe a variety of ancient societies as knowledge societies, for example, ancient Israel, which was a society structured by its religious law like Tora-knowledge. Ancient Egypt was a society in which religious, astronomical and agrarian knowledge served as the organizing principle and the basis of

authority (also Adelstein and Clegg 2014). *Contemporary society* may be described as a knowledge society based on the penetration of all its spheres of life by knowledge. Marxist theories of society have always assigned decisive importance to the forces or means of production for societal development since "man's understanding of nature and his mastery over it by virtue of his presence as a social body . . . appears as the great foundation-stone (*Grundpfeiler*) of production and of wealth," so that general knowledge becomes a direct force of production (Marx [1939–1941] 1973: 705). Contemporary Marxist theories, especially through the notion of the *Scientific-Technological Revolution* developed by Radovan Richta and others, have analyzed scientific and technical knowledge as the principal motor of change. Max Weber's seminal inquiry into the unique features of Western civilization stresses the pervasive use of reason to secure the methodical efficiency of social action (Max Weber discusses both the advantages and dangers of rational and rationalized societies: In his *Protestant Ethic and the Spirit of Capitalism* Weber argues that Puritanism had contributed to an emphasize of reason and rationality (in particular: efficiency). While this development has unquestioningly fostered the modernization of Western societies when rationalist thought and new modes to efficiently organize labor swept aside traditional feudal systems, it simultaneously created an Iron Cage (*stahlhartes Gehäuse)* of an ever more rationalized bureaucracy (Weber 1992: 123).) The source of rational action and, therefore, of rationalization is found in particular intellectual devices. The theory of *industrial society*, as developed by Raymond Aron (1962), which encompasses both socialist and capitalist forms of economic organization, stresses first and foremost the extent to which science and technology shape the social organization of productive activities and, therefore, indirectly other forms of life in society. More recent theories of *post-industrial society* and similar efforts forecasting the course of social evolution of industrial society, in particular those by Daniel Bell (1973), have elevated *theoretical* knowledge as the axial principle of society.

We plan to proceed in a number of steps: (a) we discuss concept of knowledge societies both in everyday life and in social science; (b) we address the concept of knowledge as a capacity to act in greater detail; (c) stress the distinctiveness of modern knowledge societies; (d) refer to more recently coined term knowledge-based-economies; (e) offer some observations about knowledge and innovation and, finally, (f) discuss the relations between knowledge and democracy.

Knowledge Societies

In everyday life, the term knowledge society first appears, as far as we can see, in the name of "benevolent" societies in England in the nineteenth Century. The purpose of one of these societies, the *Provident Knowledge Society* "under the patronage of Lord Derby, Lord Shaftesbury, and other distinguished men 'is' to make regular weekly saving a national habit, and so to increase the facilities for saving that it shall be as easy for a man to put by a small sum as it is now for him to spend that sum in beer or spirits. The Society has published a series of tracts upon *Penny Banks,*

Pensions, Insuring One's Life, and other subjects, which are intended to promote thrift and forethought among the working classes; and of these tracts many thousands have been circulated" (*The British Medical Journal*, 1875: 283; also *The Scottish Historical Review* 1920). In as much as the benevolent knowledge societies in England saw their mission to enlighten the uninformed public, especially members of the working class, there is at least some resemblance to features of the modern day knowledge societies that also rest on the broad dissemination of knowledge, information and knowledge skills throughout society.

In its contemporary, *social scientific* version, the term knowledge society and the idea that modern societies are knowledge societies are much more recent. The usage and development of the idea of that *modern society* is a knowledge society dates to the early 1970s and more prominently to the 1980s and later. One of the first social scientists to employ the term "knowledgeable society" is as we have mentioned Robert E. Lane (1966:650). He justifies the use of this concept by pointing to the growing societal relevance of *scientific knowledge* and defines a knowledgeable society, in a "first approximation," as one in which its members.

> (a) inquire into the basis of their beliefs about man, nature, and society; (b) are guided (perhaps unconsciously) by objective standards of veridical truth, and, at the upper levels of education, follow scientific rules of evidence and inference in inquiry; (c) devote considerable resources to this inquiry and thus have a large store of knowledge; (d) collect, organize, and interpret their knowledge in a constant effort to extract further meaning from it for the purposes at hand; (e) employ this knowledge to illuminate (and perhaps modify) their values and goals as well as to advance them. Just as the "democratic" society has a foundation in governmental and interpersonal relations, and the "affluent society" a foundation in economics, so the knowledgeable society has its roots in epistemology and the logic of inquiry.

Lane's conception of a knowledgeable society is coupled rather closely to the practical *pr*omises of a particular theory of science and reflects, also, the great optimism or fear, as the case may be, in the early 1960's suggesting that science would somehow allow for the possibility of a society in which common sense would be radically replaced by scientific reasoning freezing out opinions and ideologies in political conflicts (See the eagerness with which the title of Daniel Bell's monographh (1960) *The End of Ideology* was embraced as a diagnosis of the times . Bell (1988: 409–447) in a new afterword to his treatise vigerouslty opposes the interpreation of an end to ideologies in the latter part of the twentieth century.) That is, as Robert Lane stresses in his definition, members of the knowledgeable society are guided in their conduct, if only subconsciously, by the standards of "veridical truth."

The very promise Lane attached to scientific knowledge as the motor that would transform modern society into a knowledgeable society is the reason for other social scientists to reflect about the emergence of a "*technical state.*" One prominent social scientist that warned about the possibility of a technical state is Helmut Schelsky. Schelsky was one of the most eminent social scientists of the post-war era in Germany. His influence reached well beyond the narrow boundaries of academic social science. His influence was based on the distinctive understanding of the

evolution of modern society and the terms he coined to capture core cultural and socio-structural developments. The theories he offered were distinctly middle-range and do not have a grand design.

Robert Lane and Helmut Schelsky shared in the confidence that scientific knowledge will assume dominance throughout society and in the case of the political system reduce decision to technical matters. A brief quote from Schelsky [1961] 1965: 459) transports the essence of the meaning of the notion of the technical state:" The 'technical state or government' deprives . . . democracy of its substance. Technical and scientific decisions cannot be subject to democratic decision-making, for in this manner they only become ineffective." Helmut Schelsky adds what is perhaps obvious, namely once political decisions are executed based on certified scientific knowledge alone, the basic premise of democratic participation is eliminated: that is, the assumption is that reason and reasoned judgments are equitably distributed throughout society.

The knowledge referred to in many of the early theories of the knowledge society, and the groups of individuals that acquire influence and control with it, are conceptualized narrowly. There is a distinctive tendency to overestimate the efficacy of "objective" technical-scientific or formal knowledge and the immediate "performative" capacity of knowledge. The initial theories of modern society that evolved into the theory of the knowledge society lacked sufficient detail and scope in their conceptualization of the "knowledge" supplied, the reasons for the demand of more and more knowledge, the ways in which knowledge travels, the rapidly expanding groups of individuals in society who, in one of many ways, live off knowledge, the many forms of knowledge which are considered as pragmatically useful, failed to distinguish between information and knowledge, the application of knowledge to knowledge, the commodification of knowledge and the various effects which knowledge may have on social relations. Early theories of modern societies as knowledge societies where to put it succinctly far too impressed by the famous metapher "knowledge is power" (see Stehr and Adolf 2017).

Contemporary theories of knowledge societies therefore advocate a conception of knowledge and scientific knowledge that is distant to any notion associated with technological or scientific determinism, especially the one-sided or unidirectional forms of determinism. In more recent theories of the knowledge society, the constraining features of science and technology, for example, in the sense in which such forms of knowledge are presented as powerful phenomena to society are by no means underestimated. But in contradistinction to most arguments in favor of technological and scientific determinism, and the theories of society associated with such views, the critical point about actually existing knowledge societies is that knowledge in its various incarnations is not immediately performative nor is knowledge only appropriated by the powerful segments of society. Science and technology have important enabling features that increase the number of available strategies, heighten flexibility or affect the ability of the powerful to exercise control and constraining forces that limit choices, reduce options and enhance the fragility of major social institutions, limit the "power" of knowledge and impose penalties and risks (e.g., Stehr 2001; Mansell 2015).

It is therefore by no means contradictory to maintain that knowledge societies can simultaneously become more standardized and more fragile. Generally, it is important to avoid overstating the extent to which science and technology are forces that merely are means of control and regulation and therefore constrain human agency and limit social action. They do, but that is only part of their consequences. The other part is represented by the "opposite" because science and technology enter relational fields of social action and can assume quite different values or outcomes especially for opposing social forces and purposes. More knowledge but does necessarily mean more certainty (e.g., Trenberth 2010) (In their monograph *Merchants of Doubt* Naomi Oreskes and Eric Conway (Oreskes and Conway 2011: 267) assemble an impressive collection of example to demonstrate that the growth of scientific knowledge about climate change has not suspended political controversy. The availability (or manufacturing) of counter evidence can in fact contribute to the deepening of normative or ideological cleavages. This is because knowledge societies are not synonymous with scientized societies: "The protagonists of our story merchandised doubt because they realized – with or without the help of academic decision theory – that doubt works. And it works in part because we have an erroneous view of science.")

Knowledge

In order to demonstrate and appreciate fully the significance of knowledge for societies and social action generally, and for advanced societies in particular, one first has to formulate a *sociological* concept of knowledge. One must be able to differentiate between what is known, the content of knowledge, and knowing itself. What is it, then, that we know? Some examples taken from the *Oxford Dictionary of Current English* indicate the following instances: "Every child knows that two and two make four. He knows a lot of English. Do you know how to play chess? I don't know whether he is here or not." These examples show that knowing is a relation to things and facts, but also to laws and rules. In any case, knowing is some sort of participation: knowing things, facts, rules, is "appropriating" them in some manner, including them into our field of orientation and competence. A very important point, however, is that knowledge can be objectified, that is, the intellectual appropriation of things, facts and rules can be established symbolically, so that in the future in order to know, it is no longer necessary to get into contact with the things themselves but only with their symbolic representations. This is the social significance of language, writing, printing, and data storage.

Modern societies have made dramatic advances in the intellectual appropriation of nature and society. There is an immense stock of objectified knowledge that mediates our relation to nature and to ourselves. In a general sense, this advancement has been called, in other contexts, modernization or rationalization. This secondary nature is overgrowing the primary nature of humans. The real and the fictional merge and become indistinguishable; theories become facts and not vice versa, that is, facts do not police theories.

It is only after one acquires a sense of the societal significance of such opposites and oppositions that the full sociological significance of knowledge begins to emerge. Such a perspective assures that one realizes the extent to which knowledge can form the basis for authority, that access to knowledge becomes a major societal resource and the occasion for political and social struggles.

We would like to characterize knowledge as a generalized *capacity to act* and as a model *for* reality. Knowledge enables us to "set something in motion" or prevent something from occurring such as the onset of an illness. Knowledge creates, sustains and changes existential conditions. Social statistics, for example, are not merely mirrors of societal reality; they problematize social reality by showing that it could be otherwise, suggesting and representing capacities for action.

In 1948, Claude Shannon published a small volume entitled *The Mathematical Theory of Communication*. In it he explained how words, sounds and images could be converted into blips and sent electronically. While Shannon's communication model has been surpassed by ever more complex models in communication theory, it might be argued that he foretold the digital revolution in communications. Knowledge as a symbolic "system" enables people to act on the world. Based on the same general definition of knowledge, a *software program* as a protocol for organizing "information" constitutes a form of knowledge. How to capture water power, how to smelt iron and craft tools, how to increase the output of heavy soils, how to structure a state and markets, all of these activities require knowledge that form the core of the emergence of modernizing societies.

Our definition of the term "knowledge" is indebted to Francis Bacon's famous observation that *knowledge is power*, a somewhat misleading translation of Bacon's Latin phrase: *scientia est. potentia*. Bacon suggests that knowledge derives its utility from its capacity to set something in motion. More specifically, Bacon 1620 asserts at the outset of his *Novum Organum* (I, Aph. 3) that "human knowledge and human power meet in one; for where the cause is not known the effect cannot be produced. Nature to be commanded must be obeyed; and that which in contemplation is the cause is in operation the rule." The success of human action can be gauged from changes that have taken place in social and natural reality (Krohn 1981, 1987: 87–89), and knowledge acquires *distinction*, last but not least because of its apparent ability to transform reality. Knowledge is discovery. The added value of knowledge should be seen as a capacity to illuminate and to transform reality. Knowledge as an effective or productive model *for* reality, of course, requires knowledge *of* reality. Our definition of knowledge as a capacity to act, as *enabling* knowledge, resonates with the conception of the term "know-how" by Daniel Sarewitz and Richard P. Nelson. Sarewitz and Nelson (2008) define know-how as knowledge, "some articulated and some tacit, that guides the actions of skilled agents who aim to achieve a particular practical objective."

Science is not merely, as was once widely thought, the solution to the mysteries and miseries of the world; it is, rather, the becoming of a world. The idea that knowledge is a capacity for action that transforms, or even creates, reality is perhaps almost self-evident in the case of social science knowledge, but less persuasive in the case of the natural sciences. In the case of contemporary biology, however, one is

prepared to acknowledge that biological knowledge extends to the fabrication of new living systems. Biology does not simply study nature. Biology transforms and produces novel natural realities. Biology and biotechnology are closely linked. As a result, (most of) the reality we confront in modern societies, and increasingly so, arises from and embodies knowledge. Thus, knowledge is not power (in the usual sense of the word) but, at best, represents *potential power*. It is necessary, as a result, to distinguish between the possession of knowledge as a capacity to act and the ability to exercise or implement knowledge.

The *ownership* of knowledge, and thus the power to dispose of knowledge, is as a rule not exclusive. This exclusivity, however, is required by jurisprudence as the definition of property or of the institution of ownership. Formal law, as is well known, recognizes owners and proprietors; in particular, it recognizes individuals who ought to possess, but do not possess. In the eyes of the legal system, property is indivisible. It is also of no importance what concrete material or immaterial "things" are at issue. Likewise, the sociological significance of knowledge lies primarily in the actual ability to dispose of knowledge as capacity for action.

The *economic* value of knowledge is most difficult to establish. Knowledge as a capacity of action becomes embedded in products and people. As the concept intangibles, often used as a synonym for knowledge or other intellectual properties such as patents, copyrights, trademarks or design already suggests, knowledge constitutes "unseen wealth" (Blair and Wallman 2001) most complicated to monetarize directly. Proxies such as human capital, the value of patents or trademarks are employed in efforts to quantify the economic value of knowledge.

Not everybody knows everything; therefore capacities to act are stratified, that is, not equally distributed throughout society; the social mechanisms of the distribution of knowledge therefore form a core subject matter of any sociological analysis of knowledge (cf. Schütz 1964: 121). But whether knowledge always flows to the powerful or if the powerful tend to be the stratum that most likely exploits the social control attributes of knowledge should not be determined a priori but be subjected to theoretical and empirical analysis.

Access to knowledge and information is increasingly based on the emerging digital information technologies that make the flow of intangibles, the transaction costs big data, the prize of dissemination and the sharing of findings less costly and much more convenient. There are disparities within societies and among nations in their access to knowledge and information. But such gaps have narrowed in recent years. The so-called "digital divide" in the sense of access to the Internet becomes worldwide less and less significant. A knowledge-based economy will produce new forms of ineqaility. The more important gap concerns enabling knowledge skills (or, cognitive and intellectual capacities) and its societal distribution that assure that individuals and groups can effectively cope with the available massive volume of information and knowledge and productively enhance knowledge skills (cf. David and Foray 2003: 33–34; Autor and Dorn 2013; Autor 2015a). The protection of property rights to knowledge becomes more complicated given the same technologies. Demands to make knowledge a common good conflict with economic perspectives that argue for the protection of new knowledge in order to maintain incentives

to invest in future research and development (cf. Stiglitz 1999; Vazquez and Gonzalez 2016). A balance has to be found between these incompatible positions on intellectual property rights.

Information and Knowledge

Many dictionaries and scholarly treatises simply define information as a certain kind of knowledge or refer to the apparent ease with which knowledge is converted into information. A similar symmetry or conflation between information and knowledge is evident if one defines information as "knowledge reduced and converted into messages that can be easily communicated among decision agents" (Dasgupta and David 1994: 493; see also Drucker 1993: 69). In other definitions of information and knowledge, information is simply conceptualized as a subspecies, an element or the raw material of a number of knowledge forms.

Knowledge and information may be distinguished based on economic considerations or other social points of reference: the different ways in which they are produced, stored, diffused, consulted and applied, their typical carriers and the distinct social consequences they may be seen to have in society. One of the more traditional distinctions among knowledge forms is the opposition between *knowledge of acquaintance* and *knowledge-about* (in theory). The difference between knowledge of acquaintance and knowledge-about as described by William James (1890) resonates in turn with Gilbert Ryle's ([1949] 2000) distinction between *knowing-that* and *knowing-how*.

The distinctions made by James and Ryle also suggest a possible difference between information and knowledge where information becomes less penetrating and consequential, resonating with Ryle's knowing-that, a more superficial and fleeting cognizance of the attributes of a process or the instructions about an object (However, Gilbert Ryle ([1949] 2000: 56) stresses that knowing-that does not necessarily entail or typically result in knowledge-how. Here Ryle contradicts ideas of an essential link between the two analytical categories. However as Sellars argues, the opposite must be the case, that 'knowing how' entails a knowing that for 'it can be argued, that anything which can be properly called 'knowing how to do something' presupposes a body of knowledge *that*; or, to put it differently, knowledge of truth or facts' (Sellars 1963, 1).) Knowledge enables an actor, in conjunction with control over the contingent circumstances of action, to set something in motion, to (re-)structure reality or, as the case may be, to steer clear of some event, condition or failure. Knowledge allows an actor or actors to generate a product or some other outcome. But knowledge is only a necessary, and not a sufficient, capacity for action. As indicated, in order to set something into motion or generate a product or avoid something, the circumstances within which such action is contemplated and ultimately executed to take place must be subject to the control of the actor. *Knowing is*, in other words, a cognitive and collective *doing* and therefore an active accomplishment of one or multiple actor(s).

In contrast, the function of information as we would see it is both more restricted and more general. Information is something actors have and get. It can be reduced to "taking something in." Information can be condensed into quantifiable forms. It is therefore possible and sensible to conclude that someone has more information than someone else. It is much more difficult and contentious to conclude that someone commands more knowledge than someone else. In its compacted form, information can migrate more easily. The production of Information does not as a rule require sophisticated cognitive skills and also places fewer intellectual demands on potential users. For the most part, information is straight away productive, e.g., a train schedule represents information and is immediately useful to the traveller. Further excellent examples of information are price advertising and other market information, such as the availability of products (*signalling* function). Such information is easy to get, unproblematic to have, often robust, and can certainly be promptly useful. In the context of modern economy and in other social institutions, information is very general and widely available but the consequences of having this information as such are minimal, you cannot make the train move.

We are able to generalize now, and conclude that knowledge refers to and specifies attributes of a *process* or input whereas information refers to attributes of a *product* or output (state). It might now be clearer why we distinguish knowledge and information in this manner. As Charles Lindblom (1995: 686) explains with respect to the attributes of commodities and services and the decisions consumers make about commodities and services: In many instances in the market place, "how and where the refrigerator was made, whether the work force was well treated, whether the process produced harmful wastes, and the like, you have no control over and little knowledge of." The consumer is typically informed about the price of the fridge, its energy efficiency, life expectancy, warranty, colours, the volume it may hold, its size, and so on. None of the information provided will enable you to know anything about the process of building the refrigerator, let alone convey the ability to construct it yourself or extent your life expectancy.

Advanced Knowledge Societies

Theories of advanced knowledge society do not argue that knowledge societies become uniform social and intellectual entities and that social change follows some "linear" process. Theories of advanced knowledge societies allow, for example, for the co-existence, even interdependence, of historically distinct forms of social organization and thought. Knowledge societies do not spell the end of ideology or irrationality. Nor is scientific knowledge, as a cultural ensemble, the only a way of deciphering the world; as a model for the world certified scientific knowledge compete with other, persisting forms of knowledge in everyday life and in many social institutions such as the state, education, the economy or religion. Traditional knowledge may decline in its social importance but conventional knowledge does not disappear in modern societies or is more or less completely displaced by certified scientific knowledge. What increases substantially in volume in

advanced societies is knowledge about knowledge and the need to judge knowledge claims, to be informed about the distribution of knowledge in order to gain access to specific knowledge, as may be required in everyday social contexts or exceptional circumstances (Peter Drucker's (1993: 52–53) idea that the motor of the changes and the global transmission of small c capitalism to large C Capitalism has been "a radical change in the meaning of knowledge" is illuminating: "In both West and Asia knowledge had always been seeing as applying to *being*. Almost overnight it came to be applied to *doing*. It became a resource and a utility. Knowledge had always been a private good. Almost overnight it became a public good." The new meaning of knowledge, beginning around 1880 and culminating around World War II came to be applied, as was the case in the industrial revolution not merely to tools, processes and product but to work. In the last phase after World War II knowledge is being applied to knowledge itself.)

Applied to contemporary society, the question becomes whether knowledge and *knowledge skills* (A detailed description of knowledge skills can be found in Nico Stehr (2016). The cognitive and social skills in question have some affinity to Robert Lane's (1966: 653–656) psychological "thoughtways" explicated in his "The decline of politics and ideology and the knowledgeable society.") can provide the robust principle for social hierarchies and stratification, for the formation of inequality structures, for the distribution of chances of social and political influence and for the nature of personal life and, finally, whether knowledge may also prove to be a normative principle of social cohesion and integration even though the variations and alterations in the reproduction of knowledge appear to be enormous.

Paradoxically, efforts to entrench necessity in history or eliminate chance from history have produced, at least at the collective level, it seems, its opposite. The role of chance at the collective level continues to be part of the way society comes to be organized. Knowledge societies are (to adopt a phrase coined by Adam Ferguson) the result of human action but not necessarily of deliberate human design. Knowledge societies emerge as adaptations to persistent but evolving needs and changing circumstances of human conduct. Among the most significant transformations in circumstances that face human conduct is the continuous "*enlargement*" of human action. At least since the Age of the Enlightenment and the French Revolution the potential of an almost unlimited enlargement of human action was taken-for-granted. The future was conceived to be essentially open and hence uncertain. Whether this perspective of an unrestricted openness of human action still applies in the age of the anthropocene (cf. Crutzen 2002) is under threat as the alternatives of human action are restricted by past human action.

Knowledge Economies

The emergence of modern knowledge societies signals first and foremost a radical transformation in the *structure of the economy* leading as some have argued to a form of "cognitive capitalism" (cf. Peters and Reveley 2012). As Peter Drucker (1993: 65–68), one of the pioneers of the theory of the knowledge economy points put:

"*Knowledge is the only meaningful resource today.* The traditional factors of production' – land (i.e., natural resources), labor, and capital – have not disappeared but the have become secondary . . . Knowledge is . . . applied to knowledge . . . It is being applied . . . to systematic innovation." (Furthermore, as Peter Drucker (1999: 87) also stresses, "knowledge workers must be considered a *capital asset.* Cost need to be controlled and reduced. Assets need to be made to grow . . . Employees who do manual work do not own the means of production . . . Knowledge workers, however, *own* the means of production.")

In short, there is widespread agreement among social scientists that knowledge is the core determinant of economic growth in modern societies. However, there also is a widespread disagreement about the terms of analysis. The terms "human capital," "skills," "information," "capacities" and "knowledge" applicable to all occupations, jobs, tasks and sectors of the economy are widely conflated in many of the studies. We will concentrate on what we have defined as knowledge.

Because knowledge is in many respects *unlike* traditional means of production, standard economic discourse and statistical data based on such reasoning is less appropriate for these new socio-economic realities (cf. Castells 2000: 89–92). Nonetheless, the emergence of knowledge as a primary productive force is also an extension of capitalism. The fundamental impulse that keeps the capitalist motor in motion, as Schumpeter ([1942] 1962: 83) observes, "comes from the new consumers' goods, the new method of production or transportation, the new markets, the new forms of industrial organization that capitalist enterprise creates." And the condition for the possibility of keeping the engines of the economy running is, increasingly, incremental or novel knowledge.

Productive processes in *industrial society* are governed by a number of factors, which appear to be on the decline in their significance as conditions for the possibility of a changing, particularly growing economy. In the case of work typical for the knowledge economy a steadily shrinking percentage of the work force in all economic sectors is engaged in making or moving things, be it in manufacturing, farming, mining or transportation.

The common denominator of the changes in the structure of the economy seems to be a shift from an economy driven and governed, in large measure, by "material" inputs into the productive process and its organization to an economy in which transformations in productive and distributive processes are determined much more by cultural, "symbolic" or knowledge based inputs.

Cultural capital (cf. Lo 2015) or knowledge-based inputs are embedded, on the one hand, in investments "geared to the production and dissemination of knowledge (i.e., in training, education, research and development [R & D], information and coordination); on the other, investment geared to sustaining the physical state of human capital (health care expenditures)" (David and Foray 2003: 21). In as much as investments in intangible capital asset increases in the knowledge-based economy, the labor market changes; the volume of jobs in the knowledge sensitive activities in corporations and the state increases (see Acemoglu and Autor 2012; Autor 2015b).

The economy of industrial society is initially and primarily a *material economy* and then changes gradually to a monetary economy; for example, Keynes' economic

theory, particularly his *General Theory* (Keynes 1936), reflects this transformation of the economy of industrial society into an economy affected to a considerable extent by monetary matters. But as more recent evidence indicates, the economy Keynes' described now becomes a *symbolic economy* (cf. Drucker [1980] 1981: 8). The changes in the structure of the economy and its dynamics are increasingly a reflection of the fact that *knowledge* becomes the leading dimension in the productive process, the primary condition for its expansion and for a change in the limits to economic growth in the developed world (However, as James K. Galbraith argues the transition towards a symbolic, knowledge based economy must not be understood a single step indicating a new stage of economic development. Arguably new knowledge is the driving force behind "inventions" and technological progress which in turn a described as the decisive factors for economic growth. Referring to Schumpeter's concept of creative destruction James Galbraith argues that the respective potentials of inventions and technology to destroy and to create have to be assessed *separately*. In Galbraith view the growth potential of new information technologies is limited when compared to the technological advancement driving the economic upswing of the industrial age. (Galbraith 2014: 138–140).) In the knowledge society, most of the wealth of a company is increasingly embodied in its creativity and knowledge. With the exception of the most standardized commodities and services, factors other than "the amount of labor time or the amount of physical capital become increasingly central" (Block 1985: 95) to the economy of advanced societies (see especially Drucker 1986 and Lipsey 1992) (These theoretical considerations are consistent with a general definition of the knowledge economy proposed by Walter Powell and Kaisa Snellman: "We define the knowledge economy as production and services based on knowledge-intensive activities that contribute to an accelerated pace of technological and scientific advance as well as equally rapid obsolescence" (Powell and Snellman 2004: 201).)

It is worth noting that discussions that stress the role of knowledge in contrast to discourse that focuses on technology and technological change as the motor of modern economic growth are not embedded in discussions that express anxieties about the societal role of knowledge, at least not to the same extent as is the case when the social consequences of technological change, for example, on the labor market or working conditions are addressed. As Mokyr et al. (2015: 43) note in a discussion of the history of technological anxieties, "it seems plausible that attitudes toward work and the work ethic itself are not hard-wired human universal, but rather a culturally conditioned set of beliefs and may not persist in the same form in the face of changes in the structure of the economy induced by technological change" (also Autor 2015b; Pratt 2015).

One of the few extensive and early empirical contributions to the analysis of the nature and the emergence of a knowledge society and the knowledge-based economy (knowledge industry) in particular more than five decades ago may be found in the work of the economist Fritz Machlup (1962, 1981, 1984). His analysis is constituted by an elaborate apparatus of empirical, often census type information about observable shifts and trends, such as in the occupational structure, intended to show that a knowledge society is indeed emerging and can therefore be documented

in its own self-exemplifying terms, that is, in a quantitative (rational) manner. The most recent data generated as part of the Machlup research program to quantify the overall expenditures for knowledge production in the United States may be found in Rubin and Huber's (1986) study. Their attempt to measure knowledge incomes and expenditures connected with commodities and services constitutes the explicit effort to extend Fritz Machlup's 1962 investigation into the proportion of the Domestic Economic Product that goes to knowledge production.

Knowledge Democracies

Liberties evolve on the basis of particular social forces; the survival of liberties may depend on other social forces, if not the same forces. But in some countries, even the highest virtues may not ensure that democratic institutions endure. In any case, there is quite a large and vibrant collection of competing hypotheses referring to distinctive requisites and conditions that make the development, intensification and persistence of democratic political systems possible. Social theories and ideas developed to account for the origins, the legitimacy, the stabilization, the distribution across the globe and the sustainability of democracies are of considerable value, not only within social science disciplines, but also especially as ideas (for example, "democracy is a desirable form of governance") in the world of politics, since they always include practical advice on how to advance the process of democratization.

Aside the persistent and still unbroken belief in societal progress, for example, of constitutional arrangements within societies (As Eric Hobsbawm notes in an interview with the Indian magazine *Outlook India* (http://www.outlookindia.com/full.asp?fodname=20041227&fname=Hobsbawm+%28F%29&sid=1), in the nineteenth century, in the world of political practice, the conviction of civilizational progress meant "growing constitutionality, and in international relations, greater civility in arrangements between states. A good example of the former was the gradual disarming of the civilian population and the limitation of coercive power to the state and its agents. Another is the aversion to torture to extract information. All states, even imperialist powers, believed that there had to be a different, and a better way to obtain information. Trial and punishment had to be operated in a different way. Let me remember how strong this tradition was. There was a time when the US did not want to have a secret service. It was born of the now quaint sounding belief that gentlemen did not read each other's letters."), liberal thinkers of the nineteenth century in particular were convinced that the widespread dissemination of knowledge constituted an emancipatory force. The perhaps uncritical trust advocated by liberal thinkers of the nineteenth century, such as John Stuart Mill or Alexis de Tocqueville, in the broader societal dispersion of knowledge as the basis for social and political progress has been subjected to considerable stress in subsequent decades, and has of course met with severe objections.

The emergence of "knowledge democracies" while portrayed as an inevitable vanishing point of advanced knowledge societies (cf. in't Veld 2010) is therefore a delicate and complicated issue. The relation between (scientific) knowledge and

development of democratic institutions remains ambivalent: Science and a growing scientific literacy of the wider population can be described as drivers for the emergence of both: democratic institutions and attitudes. However, the relation can be portrayed the other way round, that it is exactly the existence of democratic freedom which leads to a heyday of scientific thinking (Stehr 2008: 5).

The predictable ambivalence between knowledge and democracy as essentially contested concepts accounts for the difficulties to clearly estimate the impact of knowledge on the "quality" of democratic decision-making. Efforts to assess quality of democratic systems usually include a combination key or proxy variables such as "freedom," "equality," "control" and "sustainable development" (Campbell et al. 2015: 471) or "civil rights," "participation," "inequity" and "competition" respectively (Altman and Pèrez-Linán 2002: 90).

Knowledge can affect all of these dimensions of democratic order in one way or the other and the direction of this influence is difficult to anticipate, let alone to quantify and very much depends on the specific socio-historical context. In theory the transition towards knowledge democracies should increase the quality of governance since citizens would increasingly be able to evaluate political programs and hold lawmakers better accountable (cf. Landemore 2013). The use of knowledge, especially scientific knowledge bears the risk of reinforcing technocratic decision-making (Ruser 2015, 2017) thus potentially limiting civic participation and suspending political competition.

The transition towards knowledge democracies is not invariably paving the way to an enlightened state of rational debate and informed decision-making. Studies aiming at estimating the impact of knowledge and information, therefore, have to carefully scrutinize the selection of the proxies that stand for democratic order and to reflect on how knowledge in general and scientific knowledge in particular is affecting and altering the internal balance of such crucial features as "freedom," "control," "participation" (Stehr 2016), "collective intelligence" (cf. Landemore, 2012, 2013) or "equality" (Campbell et al. 2015: 474).

Cyber-Democracy

The discussion of the societal role of the Internet has not only focused on "access, technological determinism, encryption, commodification, intellectual property, the public sphere, decentralization, anarchy, gender and ethnicity" but also the political repercussions of the digital world (cf. Poster 1995). Assuming that the state or corporations do not shape the Internet entirely in their image and places of digital liberty remain, is cyber-democracy perhaps the next step, the next level of development for knowledge democracies? Visions of the advent of the "netizen" (internet citizen), the virtual representation of Lincolns "the people where expressed at a time when the idea that the net community could "include all citizens (Ogden 1994: 719) was far from being utter reality and at a moment when the internet was seen as a rare example of a true, modern, functional anarchy (Ogden 1994: 720). The vision was that of an ideal Jeffersonian type of democracy:

> In this vision of a cyberdemocracy, people can live (physically) almost anywhere they wanted without forgoing opportunities of association or useful and fulfilling employment by 'telecommuting' to their 'virtual offices' or at 'Cyberspace Inns' all on the electronic superhighway. (. . .) Because of the free flow of information across local, state, regional and national boundaries access to government information at all levels become a 'right' of all netizens in the facilitation of their informed participation in the democratic process at whichever level they so choose (Ogden 1994: 723).

Twenty years later not too much of this optimistic vision remained. Despite dramatically increased access, the talk about the first generations of digital natives and the ever more growing importance of social networks democracy apparently could not benefit form these developments. Colin Crouch (2004) sees democracies reduced to *Post-Democracies* maintaining a semblance of true participation only. Peter Mair (2013) diagnoses the end of modern party democracy and roots the hollowing out of western democracy in a widespread 'citizen disengagement' (Mair 2013: 20–21).

Apparently the formula: the emergence of knowledge societies plus increased and simplified access to the world wide web equates to cyber-democracy and improved participation does not appear to be effective, for the time being. It is with this cautionary note in mind that Matthew Hindman (2009: 68) demonstrates empirically that the Internet to date has not increased political participation and mobilization in the conventional sense nor has it broadened political discourse.

Conclusion

In this contribution we outlined the emerging of modern knowledge societies and discussed the implications and consequences of the advent of knowledge-based economies and knowledge democracies. Accordingly the focus was on an understanding of the core concept of knowledge itself. Knowledge represents a capacity to act. It is not immediately performative or persuasive. Nor will "Knowledge" be a "great equalizer" forcing modern knowledge societies to converge into homogeneous social entities, for example, in terms of inequality structures, let alone will become rational social structures enabling technocratic governing, for instance.

Knowledge economies can be aptly characterized by the transition from material to symbolic economies, with knowledge becoming a leading dimension in the productive process. The generation of additional productive results and profits is highly dependent on the manipulation, distribution and processing of "symbols" and information or in words of Friedrich Hayek on the "knowledge creating function of markets" (Gray 2015). However, knowledge-based economy does not represent the abolition of capitalism.

The relation between knowledge and the development of democratic institutions is politically significant but remains ambivalent. Optimistic interpretations, which emphasize that scientific literacy and knowledge/information are drivers towards a more democratic society tend to overemphasize the role of modern communication technologies as a proxy for the advent of a cyber-democracy, that promises even

greater (digital) liberties and enhanced political participation. The Internet has neither created a free global public sphere nor has it promoted democracy at a global scale. With regard to some of the gloomier diagnoses of post-democratic developments (Crouch 2004), the resurgence of authoritarian political sentiments (Stehr 2015) or the widespread disengagement of the citizens (Mair 2013), the future of democracy in advanced knowledge societies remains to be played out in reality. Both hopes and reservations are in order.

The transition to knowledge society is not without serious problems. For example, the likelihood in the not too distant future of a permanent loss of full employment is one of the salient features of an economy in which the major source of added value is knowledge and in which ever more production will be possible with less labor power.

The promise, challenge and the dilemma knowledge societies pose for every individual derives from the need to cope with and even welcome, greater transience and volatility, the recognition that uncertainty is a necessary by-product of the search for any elimination of disagreements, and the need to accept the transitoriness of virtually all social constructs. Efforts to arrest or reverse these processes are likely to result in conditions that are worse than the alleged disease.

The increased *fragility of modern society* (see Stehr 2001) also raises new moral questions, including the issue of political responsibility for what some observers depict as political stagnation in some countries. In many countries and multinational units, for example, economic stagnation in light of unprecedented levels of unemployment and other social and economic ills would be widely diagnosed and ascribed to the governments of the day. The inability of states to devise and implement policies is typically the result of rather mundane political constraints such as endemic conflicts among vested interest of coalition partners, contingencies driven by election considerations, international developments, or even the conviction that renewal carries too many risks. Whatever the significance of borders, knowledge societies do not present a cure for healing stratified forms of life; the question of how much social and cultural inclusion or exclusion is warranted and practiced remains open.

As far as the future of knowledge societies is concerned, we would be surprised if we are not surprised. We are only able to rely on not being able to rely on the future.

References

Acemoglu, D., & Autor, D. (2012). What does human capital do? A review of goldin and Katz's the race between education and technology. *Journal of Economic Literature, 50*, 426–463.

Adelstein, J., & Clegg, S. (2014). And rewind! Recycling discourses of knowledge work and knowledge society. *Management and Organizational History, 9*(1), 3–25. https://doi.org/10.1080/17449359.2013.821023.

Altman, D., & Pèrez-Linán, A. (2002). Assessing the quality of democracy: Freedom, competitiveness and participation in eighteen Latin American Countries. *Democratization, 9*(2), 85–100.

Aron, R. (1962). *Eighteen lectures on industrial society*. New York: Free Press.

Autor, D. H. (2015a). Skills, education, and the rise of earnings inequality among the 'other 99 percent'. *Science, 344*, 843–851.
Autor, D. H. (2015b). Why are there still so many jobs? The history and future of workplace automation. *Journal of Economic Perspectives, 29*, 3–30.
Autor, D. H., & Dorn, D. (2013). The growth of low-skill service jobs and the polarization of the US labor market. *American Economic Review, 103*, 1553–1597.
Bacon, F. ([1620] 1762). *Novum Organum Scientarium*. Venetiis: Typis G. Girardi.
Bell, D. (1960). *The end of ideology. On the exhaustion of political ideas in the fifties*. New York: Free Press.
Bell, D. (1973). *The coming of post-industrial society. A venture in social forecasting*. New York: Basic Books.
Bell, D. (1988). Afterword. In *The end ideology. The exhaustion of political ideas in the fifties* (pp. 409–447). Cambridge, MA: Harvard University Press.
Blair, M. M., & Wallman, S. H. M. (2001). Unseen Wealth. In *Report of the Brookings task force on intangibles*. Washington, DC: Brookings Institution.
Block, F. (1985). Postindustrial development and the obsolescence of economic categories. *Policing and Society, 14*, 416–441.
Böhme, G., & Stehr, N. (Eds.). (1986). *Knowledge society*. Dordrecht: D. Reidel Publishing.
Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493.
Castells, M. (2000). *The rise of the network society* (Vol. 1, 2nd ed.). Oxford: Blackwell.
Crouch, C. (2004). *Post-Democracy*. Cambridge: Polity Press.
Crutzen, P. J. (2002). Geology of mankind. *Nature, 415*(6867), 23.
Dasgupta, P. S., & David, P. A. (1994). Toward a new economics of science. *Research Policy, 23*, 487–521.
David, P. A., & Foray, D. (2003). Economic fundamentals of the knowledge society. *Policy Futures in Education, 1*, 20–49.
Drucker, P. F. ([1968] 1972). The age of discontinuity. In *Guidelines to our changing society*. New York: Harper & Row.
Drucker, P. F. ([1980] 1981). *Toward the next economics and other essays* (pp. 1–21). New York: Harper & Row.
Drucker, P. F. (1986). The changed world economy. *Foreign Affairs, 64*, 768–791.
Drucker, P. F. (1993). The rise of the knowledge society. *Wilson Quarterly, 17*, 52–71.
Drucker, P. (1999). Knowledge-worker productivity: The biggest challenge. *California Management Review, 41*, 79–94.
Galbraith, J. K. (2014). *The end of normal*. New York: Simon & Schuster.
Gray, J. (2015). The Friedrich hayek I knew, and what he got right – and wrong. *New Statesman*. 30 July 2015.
Grundmann, R., & Stehr, N. (2012). *Experts: The knowledge and power of expertise*. London: Routledge.
Hindman, M. (2009). *The myth of digital democracy*. Princeton University Press.
James, W. (1890). The principles of psychology (2 Vols). London: Holt and Macmillan.
Keynes, J. M. (1936). *The general theory of employment, interest and money*. London: Macmillan.
Krohn, W. (1981). Ist Wissen Macht? Zur Soziogenese eines neuzeitlichen, wissenschaftlichen Geltungsanspruchs. In K. Bayertz (Ed.), *Wissenschaftsgeschichte und wissenschaftliche Revolution* (pp. 29–57). Köln: Pahl-Rugenstein.
Krohn, W. (1987). *Francis Bacon*. München: Beck.
Landemore, H. E. (2012). Why the many are smarter than the few and why it matters. *Journal of Public Deliberation, 8*, 7.
Landemore, H. (2013). Democratic reason. In *Politics, collective intelligence, and the rule of the many*. Princeton: Princeton University Press.
Lane, R. E. (1966). The decline of politics and ideology in a knowledgeable society. *American Sociological Review, 31*, 649–662.

Lindblom, C. E. (1995). Market and democracy – Obliquely. *PS Political Science & Politics, 28*, 684–688.
Lipsey, R. G. (1992). Global change and economic policy. In N. Stehr & R. V. Ericson (Eds.), *The culture and power of knowledge: Inquiries into contemporary societies* (pp. 279–299). Berlin/New York: de Gruyter.
Lo, A. W. (2015). The Gordon Gekko effect: The role of culture in the financial industry. NBER Working Paper w21267. http://www.nber.org/papers/w21267
Luhmann, N. (1990). *Die Wissenschaft der Gesellschaft*. Suhrkamp: Frankfurt am Main.
Machlup, F. (1962). *The production and distribution of knowledge in the United States*. Princeton: Princeton University Press.
Machlup, F. (1981). *Knowledge and knowledge production*. Princeton: Princeton University Press.
Machlup, F. (1984). *The economics of information and human capital*. Princeton: Princeton University Press.
Mair, P. (2013). Ruling the void. In *The hollowing of western democracy*. London/New York: Verso.
Mansell, R. (2015). Futures of knowledge societies – Destabilization in whose interest. *Information, Communication & Society, 18*, 627–643.
Marx, K. (1939–1941). *Grundrisse der Kritik der politischen Ökonomie*. Frankfurt am Main: Europäische Verlagsanstalt.
Mokyr, J., Vickers, C., & Ziebarth, N. L. (2015). The history of technological anxiety and the future of economic growth: Is this time different? *The Journal of Economic Perspectives, 29*, 31–50.
Ogden, M. R. (1994). Politics in a parallel universe: Is there a future for cyberdemocracy? *Futures, 26*, 713–729.
Oreskes, N., & Conway, E. M. (2011). *Merchants of doubt*. London/New Delhi/New York/Sydney: Bloomsbury.
Peters, M. A., & Reveley, J. (2012). Retrofitting Drucker: Knowledge work under cognitive capitalism. *Culture and Organization, 20*, 135–151. https://doi.org/10.1080/14759551.2012.692591.
Poster, M. (1995). Cyberdemocracy: Internet and the public sphere. *Internet Culture, 201*, 218.
Powell, W. W., & Snellman, K. (2004). The knowledge economy. *Annual Review of Sociology, 30* (2004), 199–220.
Pratt, G. A. (2015). Is a cambrian explosion coming for robotics. *Journal of Economic Perspectives, 29*, 51–60.
Provident Knowledge Society. (1875). *The British Medical Journal, 1*, 283.
Rubin, M. R., & Huber, M. T. (1986). *The knowledge industry in the United States, 1960–1980*. Princeton: Princeton University Press.
Ruser, A. (2015). By the markets, of the markets, for the markets? Technocratic decision-making and the hollowing out of democracy. *Global Policy, 6*, 83–92.
Ruser, A. (2017). Der (in)diskrete Charme der Technokratie. Wirtschaftskrisen, Staatskrisen und die Entdemokratisierung von Entscheidungsstrukturen. In M. Lehmann & M. Tyrell (Eds.), *Komplexe Freiheit. Wie ist Demokratie möglich?* (pp. 203–217). Heidelberg: Springer.
Ryle, G. ([1949] 2000). *The concept of mind.* Chicago: University of Chicago Press.
Sarewitz, D., & Nelson, R. (2008). Three rules for technological fixes. *Nature, 456*, 871–872.
Schelsky, H. ([1961] 1965). Der Mensch in der wissenschaftlichen Zivilisation. In H. Schelsky (Eds.), *Auf der Suche nach der Wirklichkeit:* Gesammelte Aufsätze. Düsseldorf: Diederichs.
Schumpeter, J. ([1942]1962). *Theories of democracy.* New York: Routledge.
Schütz, A. (1964). In A. Brodersen (Ed.), *Collected papers II: Studies in social theory.* The Hague: Martinus Nijhoff.
Sellars, W. (1963). *Science, perception and reality.* Atascadero: Ridgeview Publishing.
Shannon, C. (1948). A mathematical theory of communication. *The Bell System Technical Journal, 37*(379–423), 623–656.
Simmel, G. (1906). The sociology of secrecy and of secret societies. *American Journal of Sociology, 11*, 441–498.
Stehr, N. (1994). *Knowledge societies*. London: Sage.
Stehr, N. (2001). *The fragility of modern societies: Knowledge and risk in the information age*. London: Sage.

Stehr, N. (2002). *Knowledge and economic conduct: The social foundations of the modern economy*. Toronto: University of Toronto Press.
Stehr, N. (2005). Knowledge politics. In *Governing the consequences of science and technology*. Boulder: Paradigm Publishers.
Stehr, N. (2008). *Moral markets. How knowledge and affluence change consumers and producers*. Boulder: Paradigm Publishers.
Stehr, N. (2015). The inconvenience of democracy. *Nature, 525*, 449–450.
Stehr, N. (2016). *Information, power, and democracy*. Cambridge: Cambridge University Press.
Stehr, N., & Adolf, M. (2017). Knowledge. In *Is knowledge power?* London: Routledge.
Stiglitz, J. E. (1999). Knowledge as a global public good. In I. Kaul, I. Grunberg, & M. A. Stern (Eds.), *Global public goods. International co-operation in the 21st Century* (pp. 308–325). New York: Oxford University Press.
The Fenwick Improvement of Knowledge. (1920). *The Scottish Historical Review*, *17*, 219–224.
Trenberth, K. (2010). More knowledge, less certainty. *Nature Climate Change, 4*, 20–21.
Vazquez, A. M., & Gonzalez, P. A. (2016). Knowledge economy and the commons: A theoretical and political approach to post-liberal common governance. *Review of Radical Political Economy, 48*, 140–157.
in't Veld, R. J. (2010). Knowledge democracy. In *Consequences for science, politics, and the media*. Heidelberg/Dordrecht/London/New York: Springer.
Weber, M. (1992). *The Protestant ethic and the spirit of capitalism*. London/New York: Routledge.

Mining Governance Mechanisms: Innovation Policy, Practice, and Theory Facing Algorithmic Decision-Making

25

Annalisa Pelizza and Stefan Kuhlmann

Contents

Abstract

The shift from governance *of* to governance *by* information infrastructures has major implications for innovation policy. With algorithmic governance, regimes of inclusion/exclusion "sink" in information infrastructures that act as decision-makers. Inclusive governance of innovation thus needs to dig deeper into technological details. This chapter focuses on one major aspect that characterizes algorithmic decision-making, namely, the overlap between policy and practice. Drawing upon the innovation dance metaphor, we ask whether any space for theory can be acknowledged when algorithmic governance tightly couples policy and practice. We first attempt to theoretically answer this question by introducing the Science and Technology Studies notion of "de-scription" as a translation of rules and behaviors from extrasomatic material devices to explicit textual instructions. We propose that space for innovation theory can be conceived of as a

A. Pelizza (✉) · S. Kuhlmann
Science, Technology and Policy Studies Department, Faculty of Behavioural, Management and Social Sciences, University of Twente, Enschede, The Netherlands
e-mail: a.pelizza@utwente.nl; s.kuhlmann@utwente.nl

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_29

descriptive activity. We then exemplify the overlapping argument against the case of blockchain technologies. Blockchains are the algorithmic software underpinning peer-to-peer electronic payment systems – the most renowned of which is Bitcoin. We argue that blockchains "inscribe trust" into software and thus constitute self-standing governance mechanisms. By analyzing a recent controversy in the Bitcoin community, we show that space for theory is more likely to emerge when a controversy arises, which requires description in order to recruit new allies. This evidence suggests that the relationship between theory and inclusion might be inverted: inclusion might not be the outcome of theory, but space for theory is the result of controversies in which opposite factions carry out recruitment strategies.

Keywords
Governance of innovation · Inclusion · Innovation policy · Innovation practice · Innovation theory · Innovation dance · Governance by information infrastructures · Algorithmic governance · Blockchain · Bitcoin · Script · Description · Controversy · Strategic intelligence

Introduction: The ICT-Mediated Inclusion Challenge for Governance of Innovation

The concept of innovation policy is built on the assumption that "innovation" – a perceived or intended process of material, social, and often also cultural change, incremental, or disruptive – can be "governed" (Kuhlmann 2013, p. 985). How to design governance of innovation in a way that it recognizes less represented actors, and facilitates their participation, is a key concern of contemporary innovation policies (Borrás and Edler 2014; Lundvall and Borrás 2005; Smits and Kuhlmann 2004). Broader inclusion is seen as positively affecting the directionality of new policies, the extent to which new actors can be involved (De Saille 2015; Kuhlmann et al. 2016), and even the same definition of what "grand challenges" are (Kuhlmann and Rip 2014).

A contribution to inclusive governance of innovation comes from information and communication technologies (ICTs). Since their mass adoption in early 1990s, ICTs' relationship with the governance of innovation has been mainly framed in two ways: either by looking at ICTs as powerful tools to foster democratic debate, or as emergent technologies in need of governance. In the first case, ICTs have been conceived of as a key asset to support participative policy innovation, under the rhetoric of the "Internet revolution" and, in the second case, as a technological domain that needs ad hoc governance tools.

However, as the backbone of our technology-dense societies, ICTs are never neutral tools but rather active participants in shaping actors and governance. Algorithmic software, for example, has the potential to "inscribe" sensitive decisions in technical details. As Kitchin has recently pointed out, "we are now entering an era of widespread algorithmic governance, wherein algorithms will play an ever-increasing

role in the exercise of power, a means through which to automate the disciplining and controlling of societies" (Kitchin 2016, p. 2). In this regard, a growing literature at the intersection of media studies and science and technology studies (STS) is pointing out how regimes of inclusion and exclusion "sink" in information infrastructures that not only sort and filter information but can also act as full-blown decision-makers (Beer 2009; Introna and Nissenbaum 2000; Gillespie 2014).

Given ICTs' pervasiveness in our techno-social environments, this "sinking" has had major consequences for what was traditionally framed as "cyber democracy," which is the "kinds of relations occurring within (the Internet) which suggest new forms of power configurations between communicating individuals" (Poster 1997). First, the embeddedness of decision-making in algorithmic governance reveals that the "Internet sphere" has long ceased to be a separate domain of society. Second, it shows that individuals are not the only or the pivotal actors of those relationships. At the same time and for these very reasons, inclusive governance of innovation cannot avoid taking into account contemporary algorithmic conditions of knowledge production and decision-making (Hoppe 2010).

While algorithms can be conceived of as omnipresent technologies not only for knowledge production but also for decision-making, how these technologies in turn affect the directionality of innovation is an under-investigated field of reflection. A similar endeavor should take into account not only the multiple ways in which ICTs can support the inclusion of heterogeneous types of knowledge in innovation processes (i.e., "governance of technology,") but also how algorithmic innovation itself is productive of new regimes of inclusion/exclusion, forms of knowledge, and governance patterns (what we call "governance by technology,") that in turn affect the directionality of broader innovations.

This chapter aims to contribute to a similar endeavor by focusing on one major aspect that characterizes algorithmic knowledge production and decision-making, namely, the overlap between policy and practice. With this, we mean that formal rules, possibilities, and constraints cannot be disentangled from actual use and can be accessed only in practice. Another way to describe this overlap is saying that policy is "inscribed" in software, which in turn is endowed with agency.

In section "From "Governance of Technology" to "Governance by Technology"" we further elaborate the shift from governance *of* information infrastructures to the governance *by* information infrastructures, and we suggest that this shift has major implications for inclusive governance of innovation. The main argument is that code, protocols, software, and algorithms are not only technologies to be governed but also full-blown governance actors enacting regimes of inclusion/exclusion from innovation processes. Furthermore, given their invisibility, decision-making becomes inaccessible to traditional innovation policy actors. Inclusive governance of innovation is thus expected to dig deeper into technological details that are usually invisible to innovation policy actors.

This overlapping of innovation practice and policy does not seem to leave much space for innovation theory. However, innovation theory is a key "dancing partner" (Kuhlmann et al. 2010) that can unfold assumptions and rule of thumb implicit in policy and practice. Carving out a space for theory is thus paramount in order to

sustain the participation of new or underrepresented actors in innovation process. We will discuss this issue in section "The Dance Among Innovation Policy, Practice and Theory." We focus in particular on innovation theory as an open and accessible space to engage in explicit debates about guiding principles and actors to be included and on the risk that the close overlap of innovation practice and policy entailed by algorithmic governance can get rid of any role for innovation theory. We thus ask whether and how any space for theory can be acknowledged in algorithmic governance.

We first attempt to theoretically answer this question in section "Theory as Description: Introducing Script Theory" by introducing script theory and in particular the notion of "de-scription" as a translation of rules and intended behaviors from extrasomatic material devices to explicit textual instructions. We propose that the space for innovation theory we are looking for can be conceived of as a descriptive activity carried on by scholars and analysts during moments of crises and ruptures.

This understanding of theory as de-scription will be empirically tested in the next sections. In section "Cryptographic Blockchain Technologies, or of Trust Built in Consensus Algorithms" the practice/policy overlapping argument will be exemplified against the case of blockchain technologies. Blockchains are the algorithmic software underpinning peer-to-peer electronic payment systems – the most renowned of which is Bitcoin. They allow transactions between two parties, that bypass financial institutions and other intermediaries (Nakamoto 2008). They use cryptographic "proofs of work" that – we suggest – "inscribe trust" into blockchains bearing the trace of past transactions (Ethereum Community 2015). We argue in particular that blockchains constitute self-standing governance mechanisms that closely overlap innovation practice and policy, to the extent that policy cannot be disentangled from digital practices.

In section "Carving Space for Theory as De-scription" we ask whether in this tightly coupled blockchain dance, any space is left for innovation theory. Following a recent major controversy in the Bitcoin world, we show that – despite recurrent claims going in the opposite direction – some space for theory articulation is not only possible but also needed. In particular, the Bitcoin controversy over blocks enlargement reveals that theoretical articulation can be traced in the efforts to describe technical mechanisms to recruit new allies in the debate.

In section "Conclusions," we stress the theoretical and analytical gains of establishing a dialog between script theory and the innovation dance metaphor. In the light of the analysis of the blockchain controversy, we argue that space for theory is more likely to emerge when a controversy arises that requires description in order to recruit new participants that do not have experience of rules and decisions inscribed in software. This evidence also suggests that the relationship between theory and inclusion might be inverted. While governance of innovation assumes that inclusion is a much desirable result of theory, the Bitcoin controversy shows that space for theory is not created in a pacified environment, but it is the outcome of controversies in which factions carry out recruitment strategies.

From "Governance of Technology" to "Governance by Technology"

When it comes to governance of innovation, ICTs have mainly played two roles, being conceived of either as tools for democratic inclusion or as an emergent domain in need of governance. With this chapter we propose a third approach, subsumed under the label "governance by technologies."

The first strategy stresses the alleged disintermediation potential of ICTs, rhetorically depicted as crucial tools to enhance democratic participation (Dahlberg 2011). Already in the mid-1990s, Castells (1996, p. 392) praised "the extraordinary potential of computer communication networks as instruments of grassroots self-organizing and public debate at the local level." More recently, Coleman and Blumler (2009) suggested that ICTs have opened the possibilities of more direct participatory, disintermediated communication and political action.

All in all, ICTs' democratizing potential has been one of the most influent drivers of digital innovation. While the literature in this regard is endless – ranging from 1970s' bulletin board systems to early 2000s' "Web 2.0" platforms (Pelizza 2009) – it suffices here to briefly recall its discursive roots. The original rationale focuses on the possibility entailed by ICTs to bypass traditional political intermediaries. This bypassing would allow citizens to communicate louder and clearer with policy-makers, or even to take direct political action (Van Dijk 2000). As Formenti has pointed out, the disintermediation argument finds its roots in such principles as localism, individual empowerment, distrust in professional expertise, and direct commitment of individual citizens to political affairs. These principles were introduced by the Jeffersonian ideal of democratic self-governed townships in which decisions were taken during public open assemblies (Formenti 2008). Through the mediation of the 1960s and 1970s counter-culture movements, direct commitment and distrust in intermediaries were then inherited by the democratic rhetoric associated with early computer networks (Turner 2006), and later on with digital communities (Pelizza 2010a, b).

It is worth noticing that the disintermediating rhetoric does not take into account an important aspect: technical disintermediation does not need to imply political disintermediation. ICTs may bypass human intermediaries, but not intermediaries *tout court*. They can rather entail automation, that is, delegation of tasks to devices. STS analyses of practices supported by information infrastructures, for example, have shown that fewer human intermediaries in information exchanges do not necessarily entail disintermediation. They can rather reveal a delegation of tasks to techno-social artifacts that implement decisions taken elsewhere (Kuhlmann 1985; Oudshoorn 2011; Pelizza 2016). Therefore, an important issue in this case concerns which kind of participation to innovation processes can take place, when devices take over human tasks.

The second approach to the relationship between governance of innovation and ICTs conceives of the latter as technologies to be governed. The field of Internet governance (IG), for example, can be seen as an extension of technology assessment techniques in which assessment does not only concern specific technologies (e.g., the TCP/IP

protocol) but the Internet as a pervasive yet independent sphere of techno-social activity. IG research thus focuses also on the institutions established to negotiate the Internet's technical coordination (Hofmann et al. 2016).

IG studies conduct an important activity geared toward assuring free, continuous, and equal access to the Internet, especially by focusing on its technical layers. Furthermore, the most recent studies have the merit of having shown that broad stakeholder inclusion does not automatically entail democratic participation to governance mechanisms (Malcolm 2015). However, by considering the Internet as an independent sphere of governance, IG is less interested in fostering participation and inclusion in broader innovation processes. With some recent exceptions (see among others Musiani et al. 2016), IG's focus on the Internet seems to linger at the "governance of technology" level, where technology – even an encompassing definition of "technology" – remains the primary object of concern.

Given their pervasiveness in our techno-social environments, however, ICTs are never only tools nor is the Internet a sphere separated from broader techno-social phenomena. From Lawrence Lessig's formulation of "code as law" (2006) to Laura DeNardis' "protocol politics" (2009), from Bowker and Star's "infrastructural inversion" (1999) to Galloways' protocol-based "virtual bureaucracies" (2004), software, protocols, and information infrastructures have been acknowledged as governance actors shaping more or less inclusive (and included) identities.

This is clearly evident with algorithms. By ordering and sorting data, people, and behaviors out, algorithms enact regimes of inclusion/exclusion and act as full-blown decision-makers. Issue credit, for example, is based on rote algorithms. Trading algorithms take financial decisions at a speed that excludes any human supervision (Knorr-Cetina 2014) and can determine the solvency of the world's leading banks (MacKenzie 2012). But algorithms also take decisions about what is visible or not on the web (Introna and Nissenbaum 2000), regulate access to public space (Graham 2005), and determine who is who on social networks (Lovink 2013).

With the expressions "governance by information infrastructures" or, more specifically, "algorithmic governance" (Kitchin 2016), we stress this shift from conceiving of ICTs, either as a distinct "democratizing layer" added on top of existing techno-social arrangement or as a technological domain to be assessed, to seeing them as pervasive artifacts that do things.

The move toward governance by information infrastructures has major implications for inclusive governance of innovation. According to Gillespie, public relevance of algorithms unfolds along six dimensions: patterns of inclusion, cycles of anticipation, evaluation of relevance, the promise of algorithmic objectivity, entanglement with practice, and production of calculated publics (2014, p. 168). Drawing a parallel with the governance of innovation is straightforward. The first dimension may refer to the (algorithmic) choices behind who comes to be considered an innovation actor and who is excluded. Cycles of anticipation characterize innovation processes as well as algorithmic governance and can therefore be deeply influenced by the latter. The evaluation of relevance points to the criteria by which algorithms determine what is appropriate and legitimate knowledge and could thus affect the learning processes that support innovation. The promise of objectivity is expected to

black box, and therefore strengthen, the role of algorithmic decision in innovation processes. The fifth dimension refers to how actors change their practices to suit algorithms they depend on and might thus be extended to innovation stakeholders. Finally, the production of calculated publics points to how the algorithmic representation of actors performs new forms of identity and might trigger new identities for innovation actors.

All in all, acknowledging the governing potential of ICTs and algorithms raises new questions. If it is software that decides rules, norms, and behaviors, then according to which principles does it decide? How can inclusiveness of innovation processes be assured once it is algorithms that establish who can access them? If algorithms are productive of new regimes of inclusion/exclusion, which are the spaces (either physical or virtual) for debating algorithmic governance? In other words, when inclusion/exclusion regimes are established by software, inclusive governance of innovation has to dig deeper into technological details that are usually invisible and inaccessible to traditional innovation policy actors.

The following section addresses this issue in the light of the innovation dance metaphor. While at this stage, it refrains from identifying specific innovation policy, practice, and theory actors, it discusses these three functions as "dancing partners." It highlights the key role of innovation theory as a space for debating principles, actors, and modalities of algorithmic governance and thus for supporting the participation of new or underrepresented actors in innovation process.

The Dance among Innovation Policy, Practice, and Theory

Different metaphors have been developed to depict the interactions among innovation practice, policy, practice, and theory. Among these, the dance metaphor stresses the learning-based nature of innovation (Kuhlmann et al. 2010), and it is thus well equipped to account for governance by technologies.

Innovation practice, policy, and theory can be seen as "partners on a dancing floor," moving to the varying music and forming different configurations. The metaphor aims to illustrate the mutual interaction of the three forces: (i) dynamics of *innovation in practice*, the (ii) role of *public and other policies*, and (iii) the role of *innovation studies*, as "theory in action."

> Taking a closer look at the dance floor one can see two of the dancers, innovation practice and policy, arguing and negotiating about the dance and music while the third, theory – not always, but often and to an increasing extent –, provides the other two partners with arguments and sometimes also with new music: Practice and policy increasingly have expectations vis-à-vis the contribution of social science based intelligence to their dance. (Kuhlmann 2013, p. 985)

We are interested in the particular potential of theory as a "dancing partner," participating in the dance and academic discourse at arm's length to practice, and its ability to unfold assumptions and rules of thumb implicit in policy and practice.

There is a chance that theory can open spaces for debate and facilitate increased reflexivity about algorithmic governance mechanisms at work.

We want to explore this chance with the present chapter because a major implication of algorithmic governance for inclusive governance of innovation is the invisibility and inaccessibility of decision-making to traditional innovation policy actors. This invisibility can be read as an overlapping of practice and policy that does not seem to leave much space to theory. However, this lack of a space for theory risks to reduce the possibility to support the participation of new or under-represented actors in innovation process. We thus ask whether any space for theory can be carved out in algorithmic governance. A guiding question of the present chapter is how can spaces for theory be acknowledged and enabled.

Theory as Description: Introducing Script Theory

We first attempt to theoretically answer this question by introducing script theory. We propose that the space for theory we are looking for can be conceived of as a "de-scriptive" activity carried on by opposite factions during moments of crises and ruptures.

The concept of "script" refers to the instructions and modalities of action embedded in the material design of a device, or artifact. So, for example, the imperative "bring back the hotel keys before leaving" is translated or "inscribed" in the heavy weights that hotels (used to) add to room keys (Akrich and Latour 1992). A script is defined as a screenplay or scenario.

> defining space, roles and interaction rules among diverse (human and non-human) actors who come to play those roles. According to this understanding, all the decisions taken during the design stage act a delegation of capabilities and skills between the artifact, the user and an assembly of techno-social devices (*dispositifs*) that constitute their setting (Akrich 1990, p. 85) authors' translation).

Two main forms of script translation are possible: the translation of a script from a verbal form to a material device ("in-scription") and the opposite movement of script translation from an extrasomatic material device to words and speech ("de-scription"). So, for example, a speed bumper "in-scribes" in plastic the warning "slow down." The same warning, however, could be "de-scribed" with an imperative verbal form (i.e., "slow down!") by a policeman controlling vehicle circulation. Despite their symmetry, the tendency toward inscribing rules and instructions in extrasomatic devices tends to be much stronger than the opposite movement of description. Description takes place only in exceptional circumstances: "the de-scription is possible only if some extraordinary event – a crisis – modifies the direction of the translation from things back to words and allows the analyst to trace the movement from words to things" (Akrich and Latour 1992, p. 260).

Furthermore, the opposite movements of inscription and description tend to be carried out by diverse social actors and institutions through diverse forms of

knowledge and materiality. Thus, the analytical endeavor proper to scholars is a textual description of the design work (i.e., inscription) carried out by engineers:

> the aim of the academic written analysis of a setting is to put on paper the text of what the various actors in the settings are doing to one another; the de-scription, usually by the analyst, is the opposite movement of the in-scription by the engineer, inventor, manufacturer, or designer. (Akrich and Latour 1992, p. 259)

The notion of script is particularly helpful to address the functioning of algorithmic software for decision-making. In a more evident way than any other digital device, algorithms define roles and intended behaviors, and delegate capabilities and interests to them. Rules, behaviors, skills and interests are thus "in-scribed" in algorithms. When a search engine filters search results, it does so on the bases of some inscribed rules. When an e-commerce algorithm suggests the next items to buy, it is actually projecting an intended behavior. When social media platforms display friends' posts or adverts, they do so on the basis of a series of assumptions about what are users' interests and skills. At the same time, algorithms delegate tasks to other actors. So, for example, a facial recognition algorithm detecting a suspect according to a set of inscribed rules triggers an alarm to the local police, thus delegating them the task of investigating the suspect's intentions.

If we follow script theory, we can assume that in algorithmic governance, the opposite movement of de-scription does only take place when some ruptures or controversies happen. In similar critical moments instructions and norms are expected to become visible, and actors can negotiate them. We thus analytically propose to conceive of innovation theory as a space for debate that can be traced whenever a de-scriptive activity takes place. So, for example, algorithmic governance would be reversed engineered, the practice/policy coupling would be loosened, and new space for theory would emerge whenever there is a need to describe technical functioning to new stakeholders. A similar occurrence is exemplified in section "Carving Space for Theory as De-scription" with the case of peer-to-peer electronic payment systems. Before that, we introduce this innovation as a kind of algorithmic governance which inscribes trust in code, a self-standing governance system in which practice and policy overlap to the extent they cannot be disentangled.

Cryptographic Blockchain Technologies or of Trust Built in Consensus Algorithms

We address the question on whether any space for innovation theory is left by discussing one of the most disruptive contemporary innovations: the case of peer-to-peer electronic payment systems. Cryptographic payment systems allow transactions between two parties that bypass traditional financial intermediaries (e.g., banks). They do so by using consensus algorithms that "inscribe trust" into blocks of code – so-called blockchains – that bear trace of past transactions. Saying that "trust

is inscribed in code" means that it is software, not humans, that enforces a trustful behavior. For this reason, in what follows, we argue that blockchain technologies (and related currencies) couple innovation policy and practice in a way that they cannot be disentangled.

It is common knowledge in credit theory that money is first and foremost the measurement of a set of social relations, rather than a mere technical instrument (Ingham 1996, 2013). As such, it provides social relations with a standardized value and makes them comparable. Comparison is usually entrusted to a third party that mediates between two parts that do not know each other. This intermediation can be avoided when using cash currency in physical exchanges, but until a few years ago, no mechanisms existed to make payments online without a trusted party. Peer-to-peer electronic payment systems – and the digital currencies that the system issues according to predetermined rules – have been developed by transnational developer communities to address this constraint. These systems are based on a cryptographic proof that allows two parts – unknown to each other – to directly conduct a transaction without any intermediation by financial or other institutions.

A key characteristic of peer-to-peer payment systems is that transactions are computationally impossible to reverse. This feature protects both sellers and buyers from double-spending the same "block" of digital currency. It is made possible thanks to the peer-to-peer implementation of a distributed timestamp server that generates computational proofs of the chronological order of transactions. To describe the basic mechanism, we rely on the original formulation of the Bitcoin initiator, Satoshi Nakamoto. While Bitcoin (https://www.bitcoin.com/) is probably the best-known digital currency outside developers' circles, it should be mentioned that since Nakamoto's original formulation in 2008, almost 600 blockchain-based forks have been developed, as it will be discussed later on.

In the Bitcoin system, an electronic coin is defined as a chain of digital signatures. "Each owner transfers the coin to the next by digitally signing a hash (i.e., reference to) of the previous transaction and the public key of the next owner and adding these to the end of the coin" (Nakamoto 2008, p. 2). Consequently, any coin is defined by the history of its transactions, and a payee can verify the chain of ownership by verifying the signatures. What the payee cannot verify is that the payer does not double spend the money, that is, that the coin is firstly received by the payee, and nobody else. This problem is addressed through the implementation of a timestamp server that works by timestamping a block of transactions and widely publishing them. The timestamp thus publicly proves that a given transaction must have already taken place at a given time. Each timestamp includes the previous timestamp, thus forming a chain of "blocks" which is reinforced at each timestamp, hence the term "blockchain" (see Fig. 1).

The distributed timestamp server is public as it is implemented according to a peer-to-peer architecture that shares a consensus algorithm and makes use of a "proof of work." In high-level terms, the consensus algorithm can be described as a mechanism takes "inscribes trust in code" by publishing transactions. Each new transaction is broadcast to all peer nodes in the network. Each node gathers new transactions into a block and allocates CPU computational power to find an as much

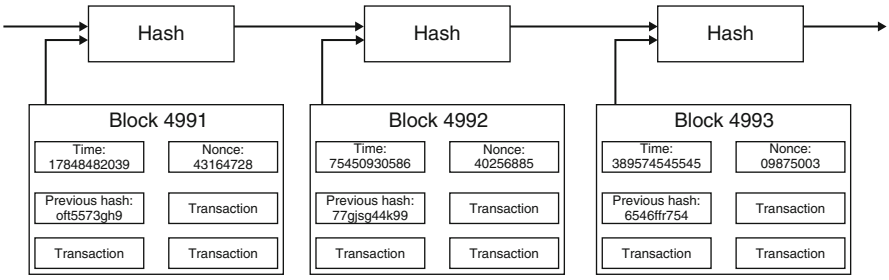


Fig. 1 Visualization of blockchain. "Hash" is the reference to the previous block

complex proof of work for its block as possible. A proof of work is a computational puzzle that in the case of Bitcoin corresponds to scanning for a value beginning with a number of zero bits. Alternative currencies have implemented different proofs of work: Primecoin, for example, requires scanning for unknown prime numbers (Primecoin 2014). This computational activity is associated with mining new materials and thus minting new coins in the Bitcoin metaphor, hence the name of network nodes as "miners."

When a node finds a proof of work, it transmits the block to all other peer nodes. These nodes accept the blocks only if all transactions in it are valid and not already spent; otherwise they reject it. When they accept a block, nodes pass to the next one by using the accepted block as the second to last. It is key to note that nodes always accept and start working on the longest chain to further extend it: if two nodes find a proof of work for the same block and thus broadcast different versions of that block, the receiving nodes will start working on the first one that they receive, but keep the second one in case it becomes longer. When the next proof of work is found and thus one of the two versions becomes longer, the shorter one will be discarded.

As the European project D-Cent has aptly summarized, "a blockchain is a timestamped ledger shared by all nodes participating in a system based on the Bitcoin protocol" (Roio et al. 2015, p. 11). The same description holds also for non-Bitcoin blockchain-based payment systems. By combining digital signatures and a peer-to-peer network using cryptographic proof of work to keep track of a public history of transactions, the blockchain system – be it Bitcoin or an alternative currency – enables users not only to bypass intermediaries but also to conduct irreversible transactions without relying on trust. "Bitcoin is a trust management system that allows for the exchange of value in a trust-less environment" (Roio et al. 2015, p. 22).

Or, to use a formulation closer to script theory, trust does not depend on interpersonal relationships between persons or institutions that know each other. Trust is indeed "inscribed" in the system architecture: (a) in the timestamp that is given to each block, assuring that at a given point in time, a transaction has already taken place; (b) in the consensus algorithm that allows nodes to collectively agree on a set of rules about the updating of the ledger; and (c) in the public character of the blockchain that is collectively and iteratively built by all peer nodes participating in

the network. The public, transparent (i.e., all transactions are visible by all participants) and symmetric (i.e., all nodes are equal peers) character of the blockchain makes "virtually impossible for anyone to stop the creation and transaction of bitcoins" (Roio et al. 2015, p. 22).

Blockchains as Self-Standing Governance Systems

Following from this description, it might be evident that blockchain architectures do not only constitute disintermediated electronic payment systems. By providing mechanisms to allocate economic value, representational rights, and membership, they aim to develop as self-standing governance systems.

Firstly, the proof-of-work algorithm constitutes the seal of equality for such a system, since any participant in the network will be equally rewarded depending on the calculating power and electricity they invested in mining new bitcoins. Therefore, in proof-of-work-based systems like Bitcoin, value is equated to CPU power. Other blockchain currencies based on a different "proof of stake" can value other aspects. Faircoin and Freicoin, for example, measure value in terms of degree of currency holding and number of transactions, respectively (Roio et al. 2015).

Secondly, blockchains do not only root economic value in specific guiding principles (i.e., CPU power, currency holding, number of transactions, etc.). They also strictly couple economic value and representational rights. The latter are expressed as rights to vote: in Bitcoin, nodes "vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism" (Nakamoto 2008, p. 8). Therefore, representational power is distributed along with economic value. In the words of Bitcoin's initiator,

> the proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. (Nakamoto 2008, p. 3)

As some commentators have noted, blockchain systems substitute bureaucratic requirements for participation – e.g., the need to be registered on a list – with technical requirements. Bitcoin, for example, substitutes "a formal barrier to participation [. . .] with an economic barrier – the weight of a single node in the consensus voting process is directly proportional to the computing power that the node brings" (Ethereum Community 2015, p. 1).

Thirdly, that blockchains aim to eventually constitute self-standing algorithmic governance systems has also shown by their defensive mechanism from nonmembers and malicious behaviors, that is, by their regimes of exclusion. The same algorithm that allocates economic value and representational rights offers also

protection from attacks. As Nakamoto has pointed out, in order to modify a block, an attacker should redo the proof of work of the whole block from scratch and then "catch up with and surpass the work of the honest nodes" (2008, p. 3). In other words, if the majority of CPU power (or of currency holding, number of transactions, etc.) is controlled by participant nodes, the chain will outpace any competing malicious chains. According to Bitcoin initiator, "taking over" an honest chain is virtually impossible with current computing systems, especially with longer chains, although quantum computing might constitute new threats (Roio et al. 2015). We will see in the next section that it was exactly when this exclusion regime was put in question that the self-consistency of Bitcoin as a governance system started to shake.

In summary, by design, blockchains aim to constitute mechanisms in which economic value distribution, political consensus building, and exclusion regimes are jointly provided by the same proof-of-work (or proof-of-stake) algorithm. These three elements correspond to three basic functions of sovereign state organization according to liberal theory: economy, politics, and security. They overlap to the point that it becomes impossible to disentangle them. In a Bitcoin system, proof of work determines at the same time the economic value of a node, its representational weight in decision-making, and who should be excluded from participation since they might want to take the chain over (i.e., those who do not run the official peer client).

That one algorithm performs these three functions at the same time is a perfect example of a technology aiming at virtual sovereignty. This is why, despite all considerations about the actual feasibility of this project (Guadamuz and Marsden 2015), we propose to conceive of blockchains as self-standing governance systems that "inscribe" in software the rules regulating value distribution, representational power, and membership exclusion.

Resorting to the innovation dance metaphor, it may be argued that blockchain technologies couple policy and practice in a way that they cannot be disentangled. The innovative practice of "mining" value for the peer-to-peer network and transferring it among peers goes hand in hand with the policy mechanism that attributes one vote to each CPU (in the Bitcoin case), to the point that distinguishing between financial practices and representational policy becomes operationally impossible.

Carving Space for Theory as De-scription

When blockchain technologies couple policy and practice in a way that they cannot be disentangled, new questions arise. As we have suggested when introducing the dance metaphor, while policy and practice can be seen engaging in a partner dance, the role of theory appears less visible. Is any space left for theory in this dance? Is any space for principles articulation possible when policy is inscribed in blockchains? This question is highly relevant in order to establish the conditions of inclusiveness of an innovation process.

As we argued in section "The Dance Among Innovation Policy, Practice and Theory," theoretical reflection is crucial to design governance of innovation in a way that it recognizes less represented actors and facilitates their participation. Space for

theorization – arenas, fora, and debates – allows explicitly addressing the inclusion/exclusion regimes entailed by technological innovation. This is recognized by some projects that are trying to develop more inclusive blockchains. According to the EU-funded D-Cent project initiator of Freecoin, for example, democratic debate is necessary to the technological development:

> the common characteristic of the different [blockchain] pilots and use-case here described is the need to strengthen the democratic debate necessary to consolidate and preserve the management of economic transactions, especially those with a social orientation, inside the local monetary circuit pilots. [. . .] Only through a democratic and participatory deliberation system, citizens can collectively define bottom-up their social needs, and inform the choices made on resource allocation and investment in social objectives and ethical criteria. This concerns the notion of "social sustainability": without participation and real democracy, local monetary circuits run the risk to remain too little, too dependent on the local political cycles, too far from the real demand that may be expressed by the local economic system. (Roio et al. 2015, p. 5)

That democratic debate is key to reinforce a currency is acknowledged, for example, by the Sol-Violette currency, a voucher-based schema experimented in Toulouse, France. Vouchers are distributed by local authorities to specific target groups, and their circulation is regulated by a bottom-up decision-making process. Since the currency is considered a common good, the governance model supports explicit (i.e., not inscribed in code) consensus building activities at every level (http://www.sol-violette.fr/).

Recalling the script lexicon introduced in section "Theory as Description: Introducing Script Theory," in what follows, we propose to look for the space of innovation theory as an activity of description. The question on whether the strict coupling of policy and practice in blockchain innovation leaves any space for theorization can methodologically be answered by looking for articulations of inscriptions and descriptions. When does the default inscription strategy leave space to descriptions? Which actors can descriptive strategy involve that are usually left out by inscription? According to script theory, inscriptions are expected to happen at the design stage, to involve mainly developers, and to be the default modality in the day-to-day use of digital currencies, at least as long as no incidents occur. Descriptions, on the contrary, are expected to take place in exceptional circumstances (e.g., at conferences, in online fora and media outlets whenever a rupture happens) and to involve not only developers but also technical and non-technical users at different levels.

In order to follow the alternation of inscriptions and descriptions in the blockchain innovation process – and thus to recognize when and under which conditions space for theory can emerge – we focus on the most diffused blockchain, namely, Bitcoin, and the major controversy that the Bitcoin community has faced since May 2015. The dispute concerns the size of the Bitcoin blocks. With the sudden interest by financial (i.e., banks and insurance companies) and high-tech companies toward the digital currency, the issue emerged, of how to scale up the software so that a quickly growing number of peer nodes could join the network. The

number of nodes and transactions the Bitcoin network can handle is related to the block size. The original design by Nakamoto established the block size as a cap on the number of transactions that can be processed by the network every 10 min. The cap was meant to ensure the involvement also of older computers in running the network, so that it was not taken over by big players able to afford last-generation computing power.

However, with the increasing number of nodes and transactions, the network started to show signs of delay that brought to unsuccessful transactions. For this reason, a coalition of actors started lobbying to raise or even remove the cap. Soon two factions emerged, even within the restricted (five) group of core developers: on one hand, those who valued Bitcoin's decentralized architecture the most, and could not accept that the funding principle of peer distribution was questioned in the name of other important but secondary principles, like transaction speed, and on the other hand, those who valued Bitcoin's enlargement the most and were willing to sacrifice Bitcoin's decentralized governance to the promise of global success as a cheaper, faster payment network than PayPal or Visa.

This dilemma revealed essential divergences about the guiding principles of the Bitcoin project, and how it should be governed. The match was conducted through an articulation of inscriptions and descriptions. On the one hand, both sides of the block size controversy tended to keep inscription as the default strategy. This is first and foremost evident in the mechanisms of vote as download. Already since its original formulation, every new release of the Bitcoin client software has been put to the vote. People downloading one or another software release essentially voted on which changes they accepted based on which version of the client they chose to run. The same voting/downloading mechanism was invoked also when the block size controversy led some developers to build a new fork, *Bitcoin XT*. This fork would have raised Bitcoin Core's block cap from 1 to 8 MB, while also adding further functionalities.

Forks are normal parts of open-source processes, where everyone can propose modification. In this sense, they constitute forms of debate that are inscribed in code. Therefore, while in principle democratic, they are scarcely accessible by noncore developers. In January 2015, 585 forks from Bitcoin Core could be counted, each of which created parallel and independent blockchains supporting alternative currencies (Roio et al. 2015, p. 16). In this regard, the novelty introduced by Bitcoin XT in fall 2015 was the fact that the new fork did not intend to set up a new currency but to continue mining and exchanging Bitcoins, only with a modified block size.

Bitcoin XT was developed without the shared consensus of the Bitcoin community and was thus highly controversial. This triggered a countermove that inscribed dissent in a malicious software, *BitKiller*, that tore down the computers that downloaded the Bitcoin XT fork with denial-of-service attacks. Even the largest US Bitcoin company, *Coinbase*, was briefly forced off-line after moving to XT. Following this line, also the counter-counter move resorted to an inscriptive strategy. In June 2015 *Coinwallet.eu*, a Bitcoin exchange, began spamming the Bitcoin Core network with spam transactions disguised as "stress tests." The whole system slowed down to the point of almost collapsing (Pearson 2015).

That inscription is the preferred default strategy by Bitcoin community members on both sides of the controversy (i.e., Bitcoin Core developers and Bitcoin XT proponents) is also shown by their vision of politics as the cause of Bitcoin's weakness:

> it never occurred to me that the thing could just fall apart because of people getting crazy and having fundamental political disagreements over the goals of the project. (Popper 2016)

> Mr. Maxwell was equally dismissive of Mr. Hearn's camp — saying that they had politicized what should have been a technical decision. (Popper 2016)

> he began politicking users to switch to his client. [. . .] He completely introduced a new level of politics to Bitcoin beyond what it had ever experienced. In addition, [he] has managed to make the scaling issue, a complex technical issue, into something that is a political litmus test, like abortion, or gun control, something that was sorely missing in a technical community. (The Bitledger 2016)

In these words, only rules and decisions that are technical – that is, inscribed in code – are unbiased, manageable, and ultimately effective. Once they unfold into political (i.e., explicit) debate, they risk to undermine the project at its roots. However, it is worth noticing that through the same words by which the two factions accuse each other of "politicking," they are actually deploying a rhetorical form of politics aimed at delegitimizing the opponent.

Yet – even in the midst of similar claims – there is evidence that space for theory and debate can emerge. From August 2015, when the Bitcoin XT fork was firstly announced by those pushing for block enlargement, the number of posts, articles, comments, and rebuts have increased in specialized outlets, public web arenas, and even mainstream newspapers. Even if accusations of censoring the controversy on the Bitcoin top discussion forum (https://bitcoin.org/en/community) were voiced by multiple sides (Haynes 2015, 2016; Popper 2016), blogs, mailing lists, social networks, and other web fora have hosted debates between the supporters of both factions. For example, "the wider community on the social media site Reddit has been eager to support the side of the debate they believe is best for the future of bitcoin" (Haynes 2015, p. 1).

Contributes from the Core side tried to describe the inner workings of the new Bitcoin XT fork with an eye to uncovering suspect surveilling functionalities (see, for example, Goat 2015), while contributes from the XT side described the technical constraints that would have shortly brought the main Bitcoin Core release to collapse.

We may thus ask when and why the default inscription strategy left room to descriptions. Following the events and debates that occurred during 2015, we suggest that the alternation of inscriptive (the default choice) and descriptive (the exception) strategies was first and foremost triggered by controversies. Without the rupture caused by the alleged need to rise the block size, not so many debates supported by descriptions of technical functioning would have probably appeared. Furthermore, we suggest that inscriptive and descriptive strategies appealed to

diverse intended actors, in a moment in which long-standing Bitcoin members' interests diverged, new actors pushed to enter, and further new actors had to be recruited to support opposite factions. We exemplify this hypothesis with a brief analysis of the posts, articles, and interviews published by the major actors of the controversy in the second half of 2015.

The Block Size Controversy Recruiting New Participants

In August 2015 through a vehement post on the *medium.com* blog, Mike Hearn, probably the most outspoken exponent of the enlargement faction, announced the Bitcoin XT fork to be released in the following fall. He gave the announcement by launching a major accusation against his opponents (identified in his words as some members of the restricted group of core developers, keepers of the Bitcoin Core) of not allowing space for debate. On the contrary, he engaged in a description of his opponents' technical arguments: "so let us instead discuss those arguments. There have been many. As each one came up, Gavin and myself have written articles analyzing them and rebutting them. Sometimes the answers were common sense, other times they were deeper and required more work, like doing network simulations" (Hearn 2015).

Compared to the previously mentioned claims opposing the technical doing to political discussion, this overture to a descriptive activity comes unexpected. Even more so since Hearn's final solution reaffirms the inscribed model of algorithmic governance. As a matter of fact, at the end of the post, the solution to the long controversy is once again delegated to software:

> This leaves one last mechanism for resolving the dispute. We can make a modified version of the software, and put it to a vote of miners via the usual chain fork logic used for upgrades. If a majority upgrade [sic!] to the new version and produce [sic!] a larger than 1 mb block, the minority would reject it and be put onto a parallel block chain. To get back in sync with the rest of the network they would then have to adopt the fork, clearly resolving the system in favour. If the majority never upgrade [sic!], the fork would never happen and the 1 mb limit would be hit. (Hearn 2015)

What is therefore the reason for a (temporary) shift to a descriptive style? Which were the needs that brought Hearn and others on his side to translate the closed algorithmic mechanisms into textual descriptions? It is Hearn himself that provides some hints at the beginning of the post.

> Such a fork has never happened before. I want to explain things from the perspective of the Bitcoin XT developers: let it not be said there was insufficient communication. Bitcoin forking is a topic that may interest many people, so this article is meant for a general audience. It doesn't assume previous knowledge of the debate. (Hearn 2015)

In his words, resorting to description is necessary to overcome possible resistances to the new fork by Bitcoin participants. Lack of communication (i.e.,

description) might be considered a reason for not adopting Bitcoin XT. Furthermore, description is necessary to recruit new participants among the "general audience." In other words, the target of this descriptive effort are not developers involved in the controversy but potential "customers" external to the Bitcoin world, who might be interested in joining not in the main Bitcoin chain, but in the newly released Bitcoin XT fork.

Hearn's enlargement strategy is evident also in his discursive attempt to stretch the definition of the Bitcoin technical community. In particular, he laments that companies' and wallet developers are not considered part of the technical community, and therefore their voice (supporting block increment) is not heard, even if they "represent many of Bitcoin's most passionate, devoted and technical people" (Hearn 2015). Resorting to description is functional for the XT proponents to expand the class of those who should be considered technical people: not only core developers and their affiliates but also client developers at corporate companies and start-ups.

A similar effort to open up the usually inscribed governance model to nonmembers of the Bitcoin community underpins also the comments of the Bitcoin Core faction. For example, a counter-post published on August 19 2015, few days after the XT announcement, has the goal "to help readers see through the bullshit to gain a clearer picture of what is actually going on. As we have stated multiple times, we are bitcoin believers, and our goal is to educate [. . .] the intellectually inclined" (Goat 2015). However, in this case, the target is not a "general audience" made of lay people but those who already have some basic knowledge and interest in Bitcoin's philosophy.

Along this line, in September and December 2015, the Bitcoin Core community organized meetings in Montreal and Hong Kong to discuss available alternatives to scale the Bitcoin architecture (Popper 2016). The goal was to "reach consensus on what should be done." Also these meetings were aimed to enlarge the members' base through open participation. Participants were expected to be not only developers but also academics (Hertig 2015), while the meetings' website reported also companies' representatives among the organizers (https://scalingbitcoin.org/hongkong2015/#about).

A fourth moment in which the two opposing parties adopted a descriptive style was in January 2016, a few months after the actual release of Bitcoin XT. In that occasion Hearn took the floor because of what he depicted as an imminent technical breakdown: "the network is on the brink of technical collapse. The mechanisms that should have prevented this outcome have broken down" (Hearn 2016). To prove this point, Hearn engaged in a description of the number of transaction and blocks reached in the previous months.

In this post Hearn also lied down explicitly that raising the block limits was aimed to recruit new users: "the community needed the ability to keep adding new users. So some long-term developers (including me) got together and developed the necessary code to raise the limit" (Hearn 2016). Besides his abovementioned allies (i.e., wallet developers, major mining pools), the new "users" that – according to Hearn – were pressing to join the network were investors, exchanges, and payment processors. What is striking here is that the term "users" is introduced to depict a set of actors

that in the orthodox Bitcoin governance model would be assimilated to the main categories of sellers and buyers.

The introduction of the term "user" – not familiar in a decentralized peer-to-peer network were every node counts for one – marks also a shift toward a different conceptualization of Bitcoin: not as a self-standing governance system anymore, in which economic value, representation, and membership are dealt with as a whole, but as a mere payment system. To give an example, Hearn provocatively described Bitcoin Core as a payments' network that:

- Couldn't move your existing money
- Had wildly unpredictable fees that were high and rising fast
- Allowed buyers to take back payments they'd made after walking out of shops, by simply pressing a button (if you aren't aware of this "feature," that's because Bitcoin was only just changed to allow it)
- Is suffering large backlogs and flaky payments
- Which is controlled by China
- Which the companies and people building it were in open civil war (Hearn 2016)

No reference is made to the representational and membership functions provided by the Bitcoin network as a self-standing governance system (see section "Blockchains as Self-Standing Governance Systems"). Here the author is recruiting "users" who might be interested in fast and cheap payment systems, not in a governance system that provides also mechanisms for political consensus building and membership recognition.

The day after this post was published, as a reaction a comment, was released on *The Bit Ledger* blog (supporting the Bitcoin Core faction). The author of this comment depicts by opposition the intended Bitcoin participant as someone interested in the governance system and not only in the payment network: "someone who put Bitcoin first. [...] People who care about bitcoin do not promote Altcoins because it's clear this would fracture Bitcoin and undermine the very method in which bitcoin secures itself" (The Bitledger 2016). In other words, this comment is oriented toward new and old Bitcoin participants that for the reason of considering the network not only a payment system but a self-standing governance system cannot be reduced to the role of "users."

In summary, the block size controversy shows a crisis that reflects deep conceptual differences in the understanding of the Bitcoin network either as a self-standing governance system or as a payment system. In the midst of this controversy, opposing factions need to recruit new actors to support them. To this end, replacing the default inscription mode with description is necessary to share algorithmic governance mechanisms with non-developers, or with developers who nonetheless have not previously taken part in core development.

The two factions also tend to address different actors through this descriptive endeavor. Bitcoin Core appeals to developers, intellectuals, and even companies, provided that they show some commitment toward the Bitcoin experiment not only as a payment system but as a self-standing governance system. On the other hand, the Bitcoin XT faction tends to appeal to more clear-cut actors, wallet developers,

investors, exchanges, and payment processors, to finish with the all-encompassing category of "users," which nonetheless does not fit the peer-to-peer character of blockchains.

It should be stressed that the fact that the two factions discursively recruited these actors does not imply that they succeeded in having them on their side nor that one of the two factions was more democratic. It shows that description as the translation of norms and rules in verbal text is more likely to take place when there is an interest in recruiting new actors to support one's own position in a controversy. That this triggers better democratic participation in innovation is all but demonstrated.

It remains that in this case, space for theory was ultimately carved out, despite the multiple claims for technical concreteness. We can conceive of theory as an elastic space triggered by controversies that shrinks with day-to-day "peaceful" use and widens with the need to recruit new actors to set the dispute. Like in any war, the battlefront is never the only key to success. Besides the line of fire against the immediate enemy, the outcome of a war can heavily depend upon the support of the civilians that are not directly involved on the battlefield.

Conclusions

The Bitcoin block size controversy shows the analytical gain of establishing a dialog between the innovation dance metaphor and script theory. By looking for the space for theory articulation as a descriptive endeavor, we have been able to detect temporary overtures to explicit debate even in the midst of recurrent bipartisan claims for technological inscription as the default strategy for controversy settling.

Space for theory is more likely to emerge when a controversy arises that requires recruiting new actors. In order to involve new participants that do not have skills or experience to understand rules and decisions so far inscribed in software, descriptions are needed to open up the inner mechanisms of algorithmic governance and put them to a vote. These are the exceptional moments when explicit debates can take place, and new actors can access them. These debates can take the shape of physical meetings like those organized by Bitcoin Core in Montreal and Hong Kong or of virtual debates going on through articles and posts in discussion fora, specialized magazines, and mainstream journals. In both cases, these descriptive efforts aim to recruit new actors to strengthen the ranks of opposing factions. By so doing, they also enlarge the participation to the innovation process.

What are the consequences of a similar understanding for inclusive governance of innovation? The block size case suggests two possible scenarios. On one hand, approaches to the relationship between theory and inclusion usually assume that inclusion is a much desirable result of theory. In this scenario, inclusive debates can take place when a space for theory is established. On the other hand, that relationship might also be inverted. We have seen in the Bitcoin controversy that space for theory in the form of explicit debate and description is the outcome of the need to include new actors to reinforce the opposite factions in a dispute. The necessity of inclusion requires translating scripts into a descriptive text and a form of materiality that is

accessible to diverse actors. In this scenario, space for theory is not created in a pacified environment that conceives of inclusiveness and democratic participation as values per se but as a result of controversies in which factions carry out recruitment strategies to overcome the opponents.

With this, we do not mean to imply that the innovation process is a constant struggle in which factions grant theory some room only when it promises a vantage point over their opponents. Rather, we aim to suggest a methodological strategy for theory actors in a landscape (i.e., algorithmic governance) where the overlap of innovation practice and policy seems to leave little room to innovation theory. We suggest that if theory aims to extend inclusion, it should not wait for proper debating fora to be established but actively engage in unfolding governance by technologies when it is more likely to succeed, that is, when controversies arise. All in all, a similar suggestion could contribute to the current debate on "strategic intelligence" (Edler et al. 2006; Padilla 2016). Strategic intelligence fora should not be seen as separate spaces for debate but could exploit the descriptive and inclusive potential of controversies, thus increasing the odds for wider inclusion even in tightly coupled algorithmic governance.

References

Akrich, M. (1990). De la sociologie des techniques à un sociologie des usages: l'impossible intégration du magnétoscope dans les réseaux cablés de première génération. *Technology and Culture, 16*, 83–110.

Akrich, M., & Latour, B. (1992). A summary of a convenient vocabulary for the semiotics of human and nonhuman assemblies. In W. E. Bijker & J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change*. Cambridge: MIT Press.

Beer, D. (2009). Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society, 11*(6), 985–1002. https://doi.org/10.1177/1461444809336551.

Borrás, S., & Edler, J. (2014). The governance of change in socio-technical systems: Three pillars for a conceptual framework. In *The governance of socio-technical systems: Explaining change*. Cheltenham/Northampton: Edward Elgar.

Bowker, G. C., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. Cambridge: MIT press.

Castells, M. (1996). *The rise of the network society: The information age: Economy, society, and culture* (Vol. 1). Oxford: Blackwell Publishers.

Coleman, S., & Blumler, J. G. (2009). *The internet and democratic citizenship: Theory, practice and policy*. Cambridge: Cambridge University Press.

Dahlberg, L. (2011). Re-constructing digital democracy: An outline of four "Positions". *New Media & Society, 13*(6), 855–872. https://doi.org/10.1177/1461444810389569.

De Saille, S. (2015). Innovating innovation policy: The emergence of "Responsible Research and Innovation". *Journal of Responsible Innovation, 2*(2), 152–168. https://doi.org/10.1080/23299460.2015.1045280.

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. Cambridge: The MIT Press.

Edler, J., Joly, P.-B., Kuhlmann, S., Nedeva, M., Propp, T., Rip, A., Ruhland, S., & Thomas, D. (2006). *Understanding "Fora of Strategic Intelligence for Research and Innovation"*. The

PRIME Forum Research Project, Report on major results, Strategic Review. Manchester: Manchester Institute of Innovation Research. https://doi.org/10.13140/RG.2.1.1696.4722.
Ethereum Community. (2015). White paper. A next-generation smart contract and decentralized application platform. Retrieved from https://github.com/ethereum/wiki/wiki/White-Paper
Formenti, C. (2008). *Cybersoviet. Utopie postdemocratiche e nuovi media*. Milano: Raffaello Cortina Editore.
Galloway, A. R. (2004). *Protocol: How control exists after decentralization*. Cambridge: MIT press.
Gillespie, T. (2014). The relevance of algorithms. In T. Gillespie, P. J. Boczkowski, & K. A. Foot (Eds.), *Media technologies: Essays on communication, materiality, and society*. Cambridge: MIT Press.
Goat. (2015). The Bitcoin XT Trojan. Retrieved from http://shitco.in/2015/08/19/the-bitcoin-xt-trojan/
Graham, S. D. N. (2005). Software-sorted geographies. *Progress in Human Geography, 29*(5), 562–580.
Guadamuz, A., & Marsden, C. (2015). Blockchains and bitcoin: Regulatory responses to cryptocurrencies. *First Monday, 20*(12). https://doi.org/10.5210/fm.v20i12.6198.
Haynes, A. (2015). Author attribution in the Bitcoin blocksize debate on Reddit. Retrieved from http://andrehaynes.me/static/AA_Reddit.pdf
Hearn, M. (2015). Why is Bitcoin forking? A tale of differing visions. Retrieved from https://medium.com/faith-and-future/why-is-bitcoin-forking-d647312d22c1#.icwedi7ou
Hearn, M. (2016). The resolution of the Bitcoin experiment. Retrieved from https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.9rjd1m4f2
Hertig, A. (2015, August 20). Bitcoin core devs in "Civil War" insist we're not getting the whole story. *Motherboard*. Retrieved from http://motherboard.vice.com/en_ca/read/bitcoin-core-devs-in-civil-war-insist-were-not-getting-the-whole-story?trk_source=recommended
Hofmann, J., Katzenbach, C., & Gollatz, K. (2016). Between coordination and regulation: Finding the governance in Internet governance. *New Media & Society*. https://doi.org/10.1177/1461444816639975.
Hoppe, R. (2010). From "Knowledge Use" towards "Boundary Work": Sketch of an emerging new agenda for inquiry into science-policy interaction. In R. in 't Veld (Ed.), *Knowledge democracy. Consequences for science, politics and media* (pp. 169–186). Berlin/Heidelberg: Springer.
Ingham, G. (1996). Money is a social relation. *Review of Social Economy, 54*(4), 507–529.
Ingham, G. (2013). Revisiting the credit theory of money and trust. In J. Pixley (Ed.), *New perspectives on emotions in finance* (pp. 121–139). London: Routledge.
Introna, L. D., & Nissenbaum, H. (2000). Shaping the web: Why the politics of search engines matters. *The Information Society, 16*(3), 169–185.
Kitchin, R. (2016). Thinking critically about and researching algorithms. *Information, Communication & Society*. https://doi.org/10.1080/1369118X.2016.1154087. Published online ahead of print on 25 Feb 2016.
Knorr-Cetina, K. (2014). What is the screens went black? The coming of software agents. In B. Geissler & O. Sonn (Eds.), *Volatile smile* (pp. 112–127). Nürnberg: Verlag für Moderne Kunst.
Kuhlmann, S. (1985). Computer als mythos. In W. E. A. Rammert (Ed.), *Technik und Gesellschaft, Jahrbuch* (Vol. 3, pp. 91–106). Frankfurt a.M./New York: Campus.
Kuhlmann, S. (2013). Innovation policies (vis-á-vis practice and theory). In E. D. Carayannis (Ed.), *Encyclopedia of creativity, invention, innovation, and entrepreneurship* (pp. 985–994). Berlin/Heidelberg: Springer.
Kuhlmann, S., & Rip, A. (2014). *The challenge of addressing Grand Challenges. A think piece on how innovation can be driven towards the "Grand Challenges" as defined under the European Union Framework Programme Horizon 2020*. Retrieved from https://ec.europa.eu/research/innovation-union/pdf/expert-groups/The_challenge_of_addressing_Grand_Challenges.pdf
Kuhlmann, S., Shapira, P., & Smits, R. (2010). Introduction. A systemic perspective: The innovation policy dance. In R. Smits, S. Kuhlmann, & P. Shapira (Eds.), *The theory and practice of innovation policy. An international research handbook* (pp. 1–22). Cheltenham: Edward Elgar.

Kuhlmann, S., Edler, J., Ordóñez-Matamoros, G., Randles, S., Walhout, B., Gough, C., & Lindner, R. (2016). Responsibility navigator. In R. Lindner, S. Kuhlmann, S. Randles, B. Bedsted, G. Gorgoni, E. Griessler, A. Loconto, & N. Mejlgaard (Eds.), *Navigating towards shared responsibility in research and innovation. Approach, process and results of the res-AGorA project* (pp. 132–155). Karlsruhe: Fraunhofer ISI.

Lessig, L. (2006). *Code: And other laws of cyberspace, version 2.0*. New York: Basic Books.

Lovink, G. (2013). *Zero comments: Blogging and critical Internet culture*. London: Routledge.

Lundvall, B. A., & Borrás, S. (2005). Science, technology and innovation policy. In J. Fagerberg, D. Mowery, & R. R. Nelson (Eds.), *The Oxford handbook of innovation* (pp. 599–631). Oxford: Oxford University Press.

MacKenzie, D. (2012). Knowledge production in financial markets: Credit default swaps, the ABX and the subprime crisis. *Economy and Society Volume, 41*(3), 335–359.

Malcolm, J. (2015). Criteria of meaningful stakeholder inclusion in Internet governance. *Internet Policy Review, 4*(4). https://doi.org/10.14763/2015.4.391.

Musiani, F., Cogburn, D. L., DeNardis, L., & Levinson, N. (Eds.). (2016). *The turn to infrastructure in Internet governance*. New York: Palgrave-Macmillan.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from http://nakamotoinstitute.org/bitcoin/

Oudshoorn, N. E. J. (2011). *Telecare technologies and the transformation of healthcare*. Basingstoke: Palgrave MacMillan.

Padilla, P. (2016). *Policy learning through strategic intelligence.* Doctoral degree, University of Twente, Enschede.

Pearson, J. (2015, December 23). Here's What the hell happened in bitcoin in 2015. *Motherboard*.

Pelizza, A. (2009). *Tracing back communities: An analysis of Ars Electronica's Digital Communities archive from ANT perspective*. Milan: University of Milano-Bicocca. Retrieved from http://www.annalisapelizza.eu/wordpress/wp-content/uploads/2015/07/9-Tracing_back_CommunitieRED.pdf

Pelizza, A. (2010a). From community to text and back. On semiotics and ANT as text-based methods for fleeting objects of study. *Tecnoscienza. Italian Journal of Science & Technology Studies, 1*(2), 57–89. Retrieved from: http://www.tecnoscienza.net/index.php/tsj/article/viewFile/36/32

Pelizza, A. (2010b). Openness as an asset: A classification system for online communities based on actor-network theory. In Proceedings of WikiSym '10, 6th International Symposium on Wikis and Open Collaboration. New York: ACM Press, pp. 8.1–8.10. https://doi.org/10.1145/1832772.1832784. Retrieved from http://dl.acm.org/citation.cfm?id=1832784&preflayout=tabs

Pelizza, A. (2016). Developing the Vectorial Glance: Infrastructural inversion for the new agenda on governmental information systems. *Science, Technology & Human Values, 41*(2), 298–321. https://doi.org/10.1177/0162243915597478.

Popper, N. (2016, January 14). A bitcoin believer's crisis of faith. *New York Times*.

Poster, M. (1997). Cyberdemocracy: Internet and the public sphere. In D. Porter (Ed.), *Internet culture* (pp. 201–218). New York: Routledge.

Primecoin. (2014). What is Primecoin? Retrieved from http://primecoin.io/about.php#what-xpm

Roio, D., Sachy, M., Lucarelli, S., Lietaer, B., & Bria, F. (2015). Design of social digital currency. Retrieved from http://www.nesta.org.uk/publications/d-cent-design-socialdigital-currency

Smits, R., & Kuhlmann, S. (2004). The rise of systemic instruments in innovation policy. *International Journal of Foresight and Innovation Policy (IJFIP), 1*(1/2), 4–32. https://doi.org/10.1504/IJFIP.2004.004621.

The Bitledger. (2016). On mike hearn, block size, and bitcoin's future. Retrieved from http://bitledger.info/on-mike-hearn-block-size-and-bitcoins-future/

Turner, F. (2006). *From counterculture to cyberculture. Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. Chicago: University of Chicago Press.

Van Dijk, J. (2000). Models of democracy and concepts of communication. In K. L. Hacker & J. van Dijk (Eds.), *Digital democracy: Issues of theory and practice*. London: Sage.

Regime Type and Sovereign Wealth Management: Implications of Cyber-Democracy on Sovereign Wealth Fund Investment Behavior

26

Juergen Braunstein

Contents

Abstract

This chapter compares broad characteristics of political systems with regard to their effects on the adaptation of ethical guidelines across sovereign wealth funds – large state owned investment funds. Reportedly sovereign wealth fund investments are driven by political imperatives, particularly if they come from non-Western economies with low democracy levels. However, if that is the case, how can we explain why some sovereign wealth funds of Western democracies adopting ethical guidelines in their investment practices? This chapter addresses this puzzle through the prism of cyberdemocracy, which emphasizes the nexus between modern technology and governance. Through a number of cases, this

J. Braunstein (✉)
London School of Economics and Political Science, London, UK
e-mail: J.Braunstein2@lse.ac.uk

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_13

chapter derives an initial hypothesis that sovereign wealth funds from countries with parliamentary systems and high levels of political freedom side are more likely to have ethical guidelines specified.

Keywords
Ethical investment guidelines · Transparency · Sovereign wealth funds

Introduction

Sovereign wealth funds (SWFs) – large state-owned investment funds – have become central actors in international finance specifically after the financial crisis 2007–2009. With an estimated volume of approximately US$ 7 trillion at the end of 2015, SWFs surpass the combined volume of hedge funds and private equity funds (SWF Institute 2015). SWFs have recently experienced very fast growth in terms of number and size. Within the SWF literature it is widely agreed that SWFs have been in existence at least since the 1950s. Within a single decade, between 2005 and 2015, assets under SWF management have increased by more than 600%, from US$ 895 billion in 2005 to US$ 5865 billion in 2014 (Rozanov 2005, p. 1; ESADEgeo Annual Report 2014, p. 103). This makes SWFs larger than the combined size of the global hedge fund and private-equity industry (*The Economist*, 17 January 2008). During the 2007/08 financial crisis, SWFs and their variation have been one of the most widely debated topics, attracting attention from economists, politicians, and the media (e.g., see Truman 2010).

The academic interest in SWFs and their variants across countries was triggered in 2005 by a short article titled "Who Holds the Wealth of Nations?" (Rozanov 2005 Rose 2008; Truman 2010; Yeung 2011; Ali and Al-Aswad 2012; Schena 2012; Chwieroth 2014; Thatcher and Vlandas 2016). The article was written in the context of trade disputes between emerging economies, most notably China, and the USA. In 2005, the state-owned China National Offshore Oil Corporation attempted to acquire two strategic US oil companies, Chevron Texaco and Unocal Cooperation; in 2006, state-owned Dubai Ports World made an offer to purchase port facilities located in the USA (Hufbauer et al. 2006). These offers were finally withdrawn because the host country had become increasingly suspicious of high-profile state-related foreign investments (Cohen 2009). The fear of capital account protectionism was aggravated by a sudden rise in SWFs.

A major concern among observers has been the underlying investment motives of SWFs in terms of whether they are driven by a political or an economics rationale. The combination of size and "novelty" has led commentators to describe SWFs as potential sources of stability or instability in the international economy. These views are related to the question of whether SWF investments are driven by politics or economics. While there are those, most notably Summers (Summers *quoted* in *The Financial Times,* 30 July 2007), who argue that SWF investments might be politically motivated and therefore destabilizing, others, such as Srinivasan (2008), highlight the stabilizing effect of long-term investments made by SWFs.

The investment activities of SWFs, and as such also their ethical investment activities, have been extensively covered and monitored by observers, most notably Bloomberg and Reuters, and think tanks, such as the Sovereign Wealth Fund Institute, and the financial press. For instance, in the period between January 2010 and August 2012, *The Financial Times* alone published 163 articles on SWFs and their investment activities. The increase in private financial monitoring was accompanied by an increase in public "political" monitoring. Major Western economies, such as the USA, Germany, and France, have introduced new or updated existing regulatory frameworks aimed at monitoring SWF investments (see Thatcher 2012). Thatcher (2012) highlights in his research that specifically strategic sectors as well as national champions are sensitive towards SWF investments. The protectionist backlashes of 2006 where Dubai Ports – a state entity of the UAE – was denied the acquisition of P&O ports in the US illustrates the sensitiveness of national policy makers and regulators towards SWF investments.

This chapter explores how regime types in a digital age affect choices concerning the adoption of ethical investment guidelines. To investigate this, the present chapter uses most likely cases (i.e., countries that have SWFs with high transparency levels). If SWF investment guidelines are driven by an economic rationale, then SWFs with similar investment mandates are expected to adopt similar investment behavior. If there is variation that cannot be explained by investment mandates and the funding sources, then this would raise further questions, such as: What drives these differences? The present study is approaching this question inductively. It offers an exploration of the effects of cyberdemocracy on state-behavior and provides a new perspective on the phenomenon of SWFs. It finds that SWFs of democratic countries frequently adopt ethical principles that guide their investments. These principles reflect the ethical principles of the respective government. Since governments can change, also these principles can change. This has important practical and theoretical implications.

It is worth highlighting that the present chapter treats ethical investment guidelines neither as a normative category (i.e., in terms of whether an investment is good or bad) nor in terms of business ethics (i.e., in terms of pursuing legal business practices and preventing improper business practices such as money laundering and protecting intellectual property rights). Instead, this chapter refers to ethics in terms of ethical investments principles that taking into account social factors in the investment decision process. A key mechanism to implement ethical investment principles relates to the "negative screening" and the exclusion of some companies/countries/sectors on specified ethical reasons such as environmental, human rights, and labor rights. The adoption of ethical investment guidelines has consequences. For example, an investor that adopts ethical guidelines through exclusion of sectors and companies limits its universe of investment opportunities, which also might have an effect on diversification attempts and return prospects. A commentator's statement that "[d]ivestment is a moral gesture, but financially, all it achieves is to make stocks cheaper for other investors with fewer scruples" suggests that ethical investors achieve only inferior return as compared to investors without ethical investment guidelines (*The Financial Times*, 29 May 2015) Commentators in the

financial press, notably representatives from *The Financial Times*, are sceptical in terms of whether funds with ethical investment guidelines outperform broader stock market indices (*The Financial Times*, 20 February 2015).

This chapter illustrates the link between regime type, ethical principles, and transparency, which is important to knowledge society. Transparency combined with high levels of political freedom allows close scrutiny of SWF investments and the expression of dissatisfaction among a country's population (see Clark and Monk 2009). Section "Cyberdemocracy and SWF Investments" introduces to the concept of cyberdemocracy and the SWF phenomenon. Section "The Puzzle of SWFs with Ethical Investment Guidelines and the Prism of Cyberdemocracy" looks at ten of the most transparent SWFs. It investigates whether SWFs similar in terms of transparency and their official mandate adopt different guidelines in terms of ethical investment. This helps evaluating whether there is variation in terms of "adoption of ethical investment guidelines" that is not systematically related to mandate and funding source.

Section "Empirical Cases, the Norwegian Pension Fund Global and the Turn to Ethics" looks at the characteristics of political systems and establishes a relationship between ethical guidelines and regime type. It investigates whether countries with similar regime types make similar choices with regard to SWFs in terms of whether to adopt ethical investment guidelines. It makes a contribution to the study of cyberdemocracy by incorporating an economic dimension and by developing initial hypotheses on the effects of regime type in a digital age on investment behavior of SWFs. Furthermore, it adds a qualitative dimension to existing large-N studies on SWF investments.

Cyberdemocracy and SWF Investments

The conceptual use of cyberdemocracy varies considerably within the discipline political science.

At a general level, cyberdemocracy refers to electronic political exchange via modern technology. Technology is often treated as an independent variable and democracy/regime type as the dependent variable. Authors looking at the effects of technology via social media networks on democratic reform (Xavier and Campbell 2014). For example, Xavier and Campbell (2014) look at the Arab Spring in Middle East. Modern technology is treated as one necessary but not sufficient condition behind the mobilization during the Arab Spring to explain the regime change (Xavier and Campbell 2014). Often, authors consider cyberdemocracy as a generic form of governance in terms of new public spaces for the purpose of governing democracy (Campbell and Carayannis 2013). They refer to "cyber" in terms of cybernetic and mean self-steering in a modern context facilitated through knowledge society. As such, cyberdemocracy is treated as something generically distinctive from other regime/types. Sometimes the concept of cyberdemocracy is

used in terms of measuring democracy quality and the trajectory of knowledge democracy in which information technology affects the creation of new types of public spaces (Carayannis and Campbell 2009, 2010, 2012).

The present chapter looks at another facet of cyberdemocracy, namely, its applicability to the investigation of the investment behavior of states. Thus far, little research has been done on the relationship between regime type and the investment behavior of SWFs in terms of whether investments are purely driven by an economic rationale. The adaptation of ethical investment guidelines constitutes a key part of this issue. A comparative analysis of countries with SWFs and the adaptation of ethical investment guidelines can reveal important new information on the role of regime type in a digitalized age and its effect on the behavior of financial institutions. Therefore, the research question is following: Is there a link between regime type in a digitalized age and the adaptation of ethical guidelines among SWFs? By drawing on a comparative case study, the present research develops an overview of regime types and the adaptation of ethical investment guidelines among SWFs.

The issue of states doing international investments in a digital age, notably via SWFs, has been receiving increasing attention. In the popular discourse, it has often been implied that SWF investments may be driven by political imperatives, especially if they come from non-Western economies with low democracy levels. If that is true, then how can we explain why some SWFs of Western democracies adopting ethical guidelines in their investment practices. The present study aims to address this puzzle through the prism of cyberdemocracy, which emphasizes the nexus between modern technology and governance.

This chapter explores the variation in terms of adopting ethical investment guidelines among SWFs through the prism of cyberdemocracy. The prism of cyberdemocracy is useful to analyze similar and different adoptions of ethical investment guidelines among SWFs with similar transparency levels located in different political systems in a digitalized age. Cyberdemocracy is conceptualized in a broad sense by referring to it as political exchange in a digitalized age. As such, cyberdemocracy can also coexist with other regime types (e.g., absolute monarchies). Regime type together with levels of political freedom plays a critical role in mediating the effects of modern technology, political exchange, and their effects on political practices in a digitalized age.

The Puzzle of SWFs with Ethical Investment Guidelines and the Prism of Cyberdemocracy

Despite similarities in their official mandates, funding sources, and transparency levels, SWFs adopt different approaches with regard to ethical investment guidelines. For example, out of the ten most transparent SWFs, we can observe differences between OECD and non-OECD economies (see Table 1). While SWFs of Norway and New Zealand have adopted explicit ethical guidelines, SWFs of Malaysia,

Table 1 Most transparent SWFs and the specification of ethical investment guidelines

SWF name	Country	Size in US$ bn	Funding source	Transparency ranking	Mandate	Ethical guidelines specified
Government Pension Fund	Norway	824.9	Commodity	10	Stabilization Future generations	**Yes**
Permanent Fund	US-Alaska	53.9	Commodity	10	Stabilization Future generations	**No**
New Zealand Superannuation Fund	New Zealand	20.2	Noncommodity	10	Future generations	**Yes**
National Pension Reserve Fund	Ireland	23.5	Noncommodity	10	Future generations	**Yes**
Future Fund	Australia	95	Noncommodity	10	Future generations	**Yes**
Temasek	Singapore	193.6	Noncommodity	10	Development	**No**
Mubadala	United Arab Emirates	66.3	Commodity	10	Development	**No**
State Oil Fund	Azerbaijan	37.3	Commodity	10	Development Stabilization	**No**
Social and Economic Stabilization Fund	Chile	15.2	Commodity	10	Stabilization Future generations	**No**
Khazanah Nasional	Malaysia	41.6	Noncommodity	9	Development	**No**

Sources: SWF Institute 2015, individual SWF reports, and SWF websites

Azerbaijan have not integrated explicit ethical guidelines in their investment framework. However, variation in terms of the adoption of ethical investment guidelines exists not only between SWFs of non-OECD and OECD countries but also within the latter group. For example, a number of SWFs from OECD countries notably Alaska/US and Chile have not adopted ethical investment guidelines. Furthermore, no systematic variation in terms of ethical investment guidelines exists that can be attributed to funding source and the official mandate. For example, both Alaska and Norway have oil funded SWFs with a stabilization and future savings mandates but both SWF differ in terms of whether they have adopted ethical investment guidelines.

Empirical Cases, the Norwegian Pension Fund Global and the Turn to Ethics

The Norwegian Pension Fund Global (NPFG) is the world's largest SWF. As of 2015, its assets under management are estimated at around US$ 900 bn. The NPFG funding source relates to oil and gas revenues. Norway's government put a tax levy of 78% on oil and gas production and other taxes and dividends from Norway's state-owned energy company Statoil (*The Financial Times*, 3 November 2014). The NPFG's purpose is to support the financing of Norway's National Insurance Scheme. As such, it addresses long-term considerations in the spending of government petroleum revenues.

The NPFG has one of the highest scores in transparency and follows ethical investment guidelines. It has published a set of general voting guidelines and information about the management of its ownership rights. As of 2015, the NPFG's ethical criteria are based on the UN Global Compact, the OECD Guidelines on Corporate Governance, and the OECD Guidelines for Multinational Enterprises. The NPFG's investments are electronically available and comprise more than 8000 companies (Bakker 2014). As such, the NPFG owns on average 1.25% of every listed company in the world (*The Financial Times,* 8 August 2013).

The international financial press watches closely divestment decisions based on ethical guidelines. Given the NPFG's massive size, the implementation of ethical investment guidelines has real-world implications. One observer highlights that "[as the NPFG] grows bigger, there is an increasing temptation to use it for non-investment goals"(*The Financial Times*, 3 November 2014). The NPFG has excluded firms that were associated with the production of antipersonnel land mines (e.g., Singapore Technologies Engineering, 26 April 2002), cluster munitions (e.g., Textron Inc., 31 December 2008), nuclear arms (e.g., Honeywell, 31 December 2005), tobacco (e.g., Philip Morris, 31 December 2009), severe environmental damage (e.g., Rio Tinto, 30 June 2008); serious violations of the rights of individuals in situation of war or conflict (e.g., Africa Israel Investments, 30 January 2014) (Regjeringen 2015a).

Norway's Parliament (Storting) established the NPFG's regulatory framework with the Government Pension Fund Act. In parliamentary systems, such as Norway, the government can be dissolved at any time and therefore tends to be more responsive to population. The Pension Fund Act describes the NPFG's legal basis and structure. The Storting has entrusted the Ministry of Finance with the formal responsibility for the NPFG's management. The Finance Minister takes final decision of whether to exclude companies or industries (*The Financial Times*, 11 November 2013). Clark and Monk statement that "[the NPFG] is not 'protected' from parliament and public opinion through statutory powers invested in its trustees" suggests that the NPFG is not a separate legal entity (Clark and Monk 2009, p. 2). The operational management is carried out by the Norges Bank – Norway's Central Bank (Regjeringen 2015b). In turn, the Norges Bank is doing this through its asset management unit: Norges Bank Investment Management. Norges Bank's Executive Board is subject to supervision from the Parliament-appointed Supervisory Council, which also appoints the Bank's auditor.

At the beginning, in the 1990s, the NPFG did not have ethical investment guidelines. Tranøy's statement that "[i]nitially the Central Bank was prone to ridicule the idea, and made it appear as the pipedream of 'irresponsible' left-leaning social democrats" suggests initial skepticism towards the adoption of ethical guidelines (Tranøy 2010, p. 191). Although discussions about the adoption of ethical principles started soon after the NPFG's creation, it was in the 2000s when an ethical investment framework was adopted (Tranøy 2010). That was in the context of regular reporting on the NPFG investments, such as in the production of land mines and in child labor (Tranøy 2010). Extensive media coverage on the NPFG's investments in the multinational TOTAL, which at that time had close links to the Burmese military regime, put significant political pressure to exclude TOTAL from the NPFG (Chesterman 2008). The Norwegian Finance Minister became increasingly exposed to public criticism (Chesterman 2008). Consequently, the Norwegian government established an ethical council to deal with the issue of controversial investments (Chesterman 2008).

For Tranøy (2010), the creation of the ethical council was a "defensive measure" in order "to pacify a domestic constituency" (Tranøy 2010, p. 178). According to Tranøy (2010), the council deflects claims against the Minister of Finance and thereby insulates the Minister against critique. This committee was created in 2002 and was headed by a legal scholar and philosopher without background in finance (Tranøy 2010). The council of ethics makes assessment of cases and advises the Ministry of Finance. More recently, environmental groups together with the Labour opposition started a debate lobbying about disinvestment from fossil fuels and environmental damaging projects (*The Financial Times,* 8 August 2013). In this context, the NPFG sold 23 palm oil companies because of environmental concerns (*The Financial Times,* 11 November 2013). According to Norway's State Secretary of Finance, "[the NPFG] belongs to the people of Norway and it's important we manage the fund in a way that ensures broad support" (*The Financial Times*, 8 August 2013).

SWFs with Ethical Investment Frameworks from OECD Countries: Australia's Future Fund, the New Zealand Superannuation Fund, the Strategic Fund of Ireland

The New Zealand Superannuation Fund (NZSF) shares a number of similarities with the NPFG. The New Zealand government uses the NZSF to save now in order to pay for the future cost of providing universal superannuation. As such, the purpose of the NZSF is to reduce the tax burden on future taxpayers of the cost of New Zealand Superannuation. The NZSF is a long-term, growth-oriented global investment fund (NZSF 2015a). The NZSF invests initial government contributions – and returns generated from these investments – internationally, in order to grow the size of the fund over the long term. With a portfolio of approximately US$ 20 bn, the NZSF is one of New Zealand's largest institutional investors. The New Zealand Superannuation and Retirement Income Act 2001 establishes clear operational independence for the Guardians of the NZSF and establishes standards of public accountability. The Guardians are responsible for investing the funds and maximizing return without undue risk to the NZSF as a whole and avoiding prejudice to New Zealand's reputation as a responsible member of the world community. The Guardians must maintain and operate the accounts in accordance with any directions given by the Minister or the Treasury (New Zealand Superannuation and Retirement Act 2001).

Like the NPFG, the NZSF is characterized by high levels of transparency and the adoption of an ethical investment framework. Environmental and social standards are integrated in the NZSF investment decision-making process (NZSF 2015b). The NZSF monitors the investment portfolio against best practice standards of the UN Global Conduct and the MSCI World Index. Companies outside this index are monitored individually. To date, the NZSF excludes a number of sectors such as the tobacco industry, producers of cluster munitions, nuclear explosive devices, and antipersonnel mines. Firms that have been excluded from the NZSF investment portfolio comprising Singapore Technologies Engineering Ltd., Honeywell, Africa-Israel Investments, Zijin Mining, and Tokyo Electric (NZSF 2015a).

In a similar fashion, the Australian Future Fund (AFF) and the Ireland Strategic Investment Fund (ISIF) have adopted ethical investment guidelines. The ISIF was created in 2014 with the purpose to invest on a commercial basis in a manner designed to support economic activity in Ireland (ISIF 2015). Thus far, the Cluster Munitions and Anti-Personnel Mines Act 2008 are the only relevant legislation concerning ethical investments (*Irish Times*, 13 August 2015). Any exclusion on the basis of ethical investment criteria has to be mandated by legislation (*Irish Times*, 13 August 2015). The AFF was established earlier in 2006 to meet unfunded superannuation liabilities. The AFF received its initial contributions from a combination of budget surpluses and from the proceeds from the sale of the government's holding of Telstra – Australia's largest telecom/media company (AFF 2015a).

Like the NPFG and the NZSF, the AFF excludes firms that are involved in the production of cluster munition, antipersonnel mines, and tobacco. In implementing

these guidelines, the AFF has excluded companies such as Singapore Technologies Engineering, Textron, and British American Tobacco (AFF 2015b). Interestingly, the AFF and the ISIF have not excluded companies whose actions and omissions constitute unacceptable risks or severe environmental damage. Unlike the NPFG, the AFF has significant exposure to companies, such as Rio Tinto, that are banned by the NPFG.

That can be partly attributed to Australia's high exposure to the mining sector (*ABC News,* 20 November 2014). Similarly, Ireland's ISIF invests into companies, such as TransCanada, that have been controversial because of severe environmental concerns (*Irish Times*, 13 August 2015).

Both Ireland and Australia are parliamentary systems which are characterized by high levels of political freedom. The AFF Board of Guardians is appointed by the Minister and is responsible for investing the assets of the AFF (2015a). The AFF governance structure was designed in a way to increase its independence from domestic politics. Clark's statement that "the term of appointment of 5 years with the prospect of renewal was expected to severer the link with the short-term political cycle" highlights the government's attempt to protect AFF board members from political pressures (Clark 2009, p. 19). Although the AFF ceded to popular public pressure in 2012 to sell out of tobacco and arms companies, it was highlighted that it will only sell out of coal assets only for financial reasons (*The Sidney Morning Herald*, 9 June 2015). Alone the AFF tobacco exposure was estimated to approximately AU $221 million. (*ABC News*, 28 February 2013). The management function of ISIF is carried out by Irelands National Treasury Management Agency. Out of its nine members, six are appointed by the Ministry of Finance for different time periods.

All of the SWFs from countries with parliamentary systems and high levels of political freedom have adopted an ethical investment framework. In parliamentary systems, governments can be dissolved at any time and therefore Ministers are responsive to population's wishes. This is reflected in the adoption of ethical investment guidelines among SWFs.

SWFs Without Ethical Investment Frameworks from OECD Countries: Alaska's Permanent Fund, Chile's Economic and Social Stabilization Fund

Unlike other OECD SWFs, the Alaska Permanent Fund (APF) has no specified ethical investment guidelines. In contrast to the NZSF and the NPFG, the APF has significant exposure to the tobacco industry (e.g., via its holdings in a number of tobacco firms such as British American Tobacco) as well as to the military/defense sector. For example, it holds significant shares in companies, notably Singapore Technologies Engineering, Rio Tinto, and Honeywell, which are excluded from the investment portfolio of the NPFG and the NZSF (APF 2015a).

The APF was established in 1976 in the context of Alaska's oil pipeline construction. Due to Alaska's high exposure to commodity price cycles, the basic idea

behind the creation of the APF was to save in good times and spend in bad times. However, the creation of the APF necessitated a constitutional amendment. Alaska's population broadly supported the constitutional amendment and the creation of the APF in a vote in 1976 (Brown and Thomas 1994). The constitutional amendment stipulated that at "least 25 percent of all mineral lease rentals, royalties, royalty sales proceeds, federal mineral revenue-sharing payments and bonuses received by the state [should be placed with the APF]" (APF 2015b). To manage the investments of the APF, the Alaska legislature established the APF Corporation. As of 2015, the AUM of the APF were estimated at around US$ 50 bn.

High levels of political freedom in Alaska's political system within the US federal system are reflected in Alaska's economic policy making and the APF. According to Brown and Thomas (1994, p. 44), this makes it very difficult to "promote any common goal on a long-term basis" with regard to the APF and Alaska's fiscal policy. Another factor relates to the APF's unique incentive structure. The APF's founding father Governor Hammond followed the idea of giving Alaska's residents a direct stake or interest in the APF by paying them an annual dividend out of its earnings (Brown and Thomas 1994, p. 41). That is an unusual practice among SWFs. Brown and Thomas' statement that the so-called APF dividend "soon became a sacred political cow" suggests that it is very risky for politicians to change the investment framework of the SWF (Brown and Thomas 1994, p. 43). The adoption of ethical investment guidelines can imply a tradeoff for the AFP's return. It is widely acknowledged that extensive exclusion based on ethical principles could harm the return and risk profile of funds (*The Financial Times*, 3 November 2014).

Similar to the APF, Chile's Economic and Social Stabilization Fund (ESSF) has no specified ethical investment guidelines in place. The ESSF provides fiscal stabilization as it allows the financing of fiscal deficits. It reduces Chile's dependency on global business cycles and revenue volatility related to fluctuations in copper price and other sources. The ESSF was created in 2007 with an initial contribution of US$ 2.56 bn from Chile's old Copper Stabilization Fund (Hacienda 2016). It receives on an annual basis the positive balance from Chile's fiscal surpluses after accounting for contributions for Chile's Pension Reserve Fund and payments of public debt (Hacienda 2016). As of 2015, AUM of the ESSF were estimated at around US$ 15 bn.

Under the Fiscal Responsibility Law, the Finance Minister is responsible for deciding on the ESSF's investment policies. The Minister of Finance is appointed by the President. This gives the Minister a degree of insulation from popular demands. Interestingly, there has been no public debate in Chile about the ESSF and ethical investment guidelines (This observation was made by Kenneth Bunker, an expert on economic policy in Chile). In turn, the Finance Minister appointed the Central Bank as the agent responsible for the operational management of the ESSF. The Central Bank invests the ESSF resources in accordance with the instructions and restrictions established by the Minister of Finance. In defining the instructions and restrictions, the Finance Minister is supported by a Financial Committee, which provides advice on the aspects related to this decision.

In presidential systems, the government is in office for a fixed term and the Minister of Finance is appointed by the President which gives him a degree of insulation. That in turn provides more effective protection of the SWF from parliament and public opinion. This is reflected in the choices about the adoption of ethical investment guidelines. SWFs from countries with presidential systems tend to have no ethical investment guidelines.

SWFs Without Ethical Investment Frameworks from Non-OECD Countries: Singapore's Temasek, Malaysia's Khazanah Nasional, the United Arab Emirates' Mubadala, the State Oil Fund of Azerbaijan

Singapore's Temasek is one of the most transparent SWFs in non-OECD countries. Temasek is one of Singapore's three state-owned asset managers. The other two are the Government Investment Corporation of Singapore and the Monetary Authority of Singapore. Temasek was established in the mid 1970s as a private exempt company with a constitutional status. As of 2015, AUM of Temasek are estimated at nearly US$ 200 bn. Temasek's investment spectrum covers a wide range of industries including energy, resources, technology, and military. Although Temasek is among the most transparent SWFs, critiques about investments of Singapore's SWFs are only carried out in public to a very limited extent. The Law of Defamation constrains the right of free speech (Mauzy and Milne 2002). The judicial system in Singapore has been regularly criticized for lack in independence, specifically in political sensitive areas.

Unlike other SWFs from countries with parliamentary systems, Temasek's investments are not guided by a specified ethical framework. Singapore has been frequently described as an illiberal democracy or a nonliberal communitarian democracy with judicial actions applied to government criticism (see Mauzy and Milne (2002). The People's Action Party has governed without interruption since Singapore independence in 1959 (Freedomhouse 2015). That is reflected in low levels of political freedom scores (see Freedomhouse (2015).

Like Singapore's Temasek, Malaysia's Khazanah Nasional has no explicated ethical investment guidelines. Its portfolio comprises some of Malaysia's largest and most important companies operating in different sectors including aviation, agriculture, food, and technology (Khazanah 2015).

Khazanah Nasional was created in 1993 with the aim of managing the transformation process of so-called government-linked companies – including flag-carrier Malaysia Airlines – into more commercially driven businesses (*The Financial Times*, 14 January 2015). Khazanah is owned by the Minister of Finance Incorporated, a body attached to the Ministry of Finance. Although in the constitutional monarchy of Malaysia freedom of expression is constitutionally guaranteed, it is restricted in practice (Freedomhouse 2015).

Similarly, Abu Dhabi's Mubadala has no specified ethical guidelines in its investment framework.

One of Mubadala's major strategic investment areas relates to the defense and advanced military maintenance sector. For example, Mubadala holds more than half of the shares of the Emirates Defence Industry Company – a leading defense manufacturing and military technology company (Mubadala 2015a). In addition, Mubadala partners with international corporations, such as Boing and Airbus (Mubadala 2015b). Interestingly these companies have been excluded from the investment portfolio of the NPFG on grounds that refer to the production of weapons that may violate fundamental humanitarian principles (NBIM 2015).

Mubadala's official mandate refers to economic diversification and it invests actively in projects with long-term value potential, and that boost the creation of new industry and infrastructure in Abu Dhabi. Abu Dhabi is governed by a constitutional monarchy with strong rulers. Although the UAE's constitution provides for some freedom of expression, the government restricts this right in practice and it prohibits criticism of the government and as such its SWF (Freedomhouse 2015).

Also, the State Oil Fund of Azerbaijan (SOFAZ) has no investment guidelines explicated with regard to severe environmental damages, the production of nuclear arms, and the tobacco industry. SOFAZ manages Azerbaijan's accumulated oil revenues with a purpose of developing and implementing projects of social-economic importance, notably in the infrastructure and energy sector such as the Heydar Aliyev Baku-Tbilisi-Ceyhan Main Export Pipeline (SOFAZ 2015a). SOFAZ is a legal entity separate from the government or central bank. SOFAZ's operation is guided by the constitution and presidential decrees (SOFAZ 2015b). The president of Azerbaijan is the "supreme governing and reporting authority" for the SOFAZ. The constitution of 1995 gives the President a strong power base with little accountability. President Aliyev's New Azerbaijan Party has dominated the political playing field since 1995. While the constitution guarantees freedom of the press, the authorities severely restrict the media in practice (Freedomhouse 2015).

Findings and Implications

The chapter finds that mandate, funding source cannot account for variation with regard to the adoption of ethical investment guidelines among SWFs. It discovers substantial variation in terms of the adoption of ethical investment guidelines among the ten most transparent SWFs. Variation occurs even among SWFs that belong to similar country groupings (i.e., within OECD countries). For example, both Alaska and Norway have oil funded SWFs with a stabilization and future savings mandates but both differ in terms of ethical investment guidelines. Norway's NPFG adopted ethical investment guidelines, whereas Alaska's AFF did not (see Table 2).

SWFs of countries with low political freedom scores are less likely to adopt ethical investment guidelines. That is because the political structures in place provide the SWF governance structure with more insulation from public opinion and from the values of their citizens. In line with this observation, this chapter finds that countries with high levels of political freedom are more likely to have SWF with explicated ethical investment guidelines. SWFs from systems with high levels of

Table 2 Most transparent SWFs, ethical guidelines, political freedom, and regime type

Country	SWF name	Ethical guidelines specified	Political freedom (Freedomhouse)	Regime type
Norway	Government Pension Fund	**Yes**	**1**	**Parliamentary system**[a]
US-Alaska	Permanent Fund	**No**	**1**	**Presidential republic**
New Zealand	New Zealand Superannuation Fund	**Yes**	**1**	**Parliamentary system**[a]
Ireland	National Pension Reserve Fund	**Yes**	**1**	**Parliamentary system**
Australia	Future Fund	**Yes**	**1**	**Parliamentary system**[a]
Singapore	Temasek	**No**	**4**	**Parliamentary system**
United Arab Emirates	Mubadala	**No**	**6**	**Constitutional Monarchy**
Azerbaijan	State Oil Fund	**No**	**6**	**Presidential system**
Chile	Social and Economic Stabilization Fund	**No**	**1**	**Presidential system**
Malaysia	Khazanah Nasional	**No**	**4**	**Constitutional Monarchy**

Sources: Data compiled by the author from SWF Institute (2015), Freedomhouse (2015)
[a]Constitutional monarchy or commonwealth elements
1 = best 7 = worst
1 = free
4 = partly free
6 = not free

political freedom giving greater affect to the values of their citizens through their investment policies.

Data reveal fine-grained differences among countries with high political freedom scores. Interestingly, all of the SWFs from countries with parliamentary systems and high levels of political freedom have adopted an ethical investment framework (see Table 3). In parliamentary systems, governments can be dissolved at any time and therefore it is more responsive to its population. In presidential systems, the government is in office for a fixed term and the Minister of Finance is appointed by the President, which gives him a degree of insulation. This provides more effective protection of the SWF from parliament and public opinion. That is reflected in the choices about the adoption of ethical investment guidelines. SWFs from countries with presidential systems tend to have no ethical investment guidelines. Based on these findings, we are able to formulate an initial hypothesis: SWFs of countries with parliamentary systems and high levels of political freedom are more likely to adopt ethical investment guidelines.

The findings of this chapter have a number of policy relevant implications. The recent adoption of ethical investment principles among SWFs should not alarm

Table 3 Most transparent SWFs/countries, political systems, and level of political freedom

		Political freedom	
		Low	*High*
Political system	*Parliamentary*	Temasek (Singapore)	NPFG (Norway) AFF (Australia) NZSF (New Zealand) ISIF (Ireland)
	Presidential	SOFAZ (Azerbaijan)	APF (Alaska) ESSF (Chile)
	Monarchy	Mubadala (Abu Dhabi) Khazanah (Malaysia)	n.a.

policy makers, and investors, but it raises a number of policy relevant issues. In the current debate, SWFs of nondemocratic countries are frequently associated with political driven motives. However, all of the SWFs which have applied over the recent years – ethical – non economic investment principles coming from Western democratic countries. To understand the adaptation of ethical investment guidelines, more focus has to be put on the link between regime type and levels of transparency.

Conclusion

Cyberdemocracy refers to a broad spectrum of topics, which are connected to economic and political development in a digitalized age. One of these topics refers to the investment behavior of SWFs in a digitalized context. Regime types in combination with information and communication technology can affect the investment spectrum of SWFs. As such, cyberdemocracy raises challenges as well as opportunities for state asset managers.

This chapter has started with the puzzle of variation in ethical investment guidelines among sovereign wealth funds. Drawing on the prism of cyberdemocracy, which emphasizes the nexus between information/technology and governance in a digitalized age, this chapter looked at the most transparent SWFs (i.e., SWFs that provide information about their investments). The purpose of the chapter was to investigate the link between regime type and the adoption of ethical investment frameworks among SWFs.

This chapter has compared the adoption of ethical guidelines among the most transparent SWFs and linked variation to regime type and scores of political freedom. The basic observation is that SWFs of countries with high political freedom scores are more likely to have ethical investment frameworks. Fine-grained differences occur between parliamentary and presidential systems. SWFs from countries with parliamentary systems and high levels of political freedom tend to have ethical investment guidelines, whereas SWFs from countries with presidential systems and high levels of political freedom tend to have no ethical investment guidelines.

By inductively developing hypotheses about the relationship between regime type, governance, and investment behavior, the present chapter makes a contribution to the emerging field of study on cyberdemocracy. However, the initial observations and hypothesis developed needs further testing in terms of causal mechanisms.

References

AFF. (2015a). 'About the fund', Australian Future Fund. Available: http://www.futurefund.gov.au/about_the_future_fund/outline. Accessed 12 Nov 2015.

AFF. (2015b). 'Excluded companies Australian Future Fund', Australian Future Fund. Available: http://www.futurefund.gov.au/__data/assets/pdf_file/0011/5105/2015_Aug_excluded_companies_listpdf. Accessed 13 Nov 2015.

Ali, A., & Al-Aswad, S. (2012). Persian Gulf-based SWFs and financial hubs in Bahrain, Dubai and Qatar. *World Economics, 13*(3), 109–126.

APF. (2015a). 'Investments', Alaska Permanent Fund [Homepage]. Available: http://www.apfc.org/home/Content/investments/stocksTop50.cfm. Accessed 11 Sept 2015.

APF. (2015b). 'About the fund', Alaska Permanent Fund [Homepage]. Available: http://www.apfc.org/home/Content/aboutFund/aboutPermFund.cfm. Accessed 10 Sept 2015.

Bakker, A. (2014). Norway's Sovereign Wealth Fund, Norges Bank PPP, 26 May. Available: http://www.norgesbank.no/pages/100001/age_bakker_.pdf. Accessed 12 Sept 2015.

Brown, W. S., & Thomas, C. S. (1994). The Alaska permanent fund: Good sense or political expediency? *Challenge*, 38–44.

Campbell, D. F. J., & Carayannis, E. G. (2013). *Epistemic governance in higher education. Quality enhancement of universities for development*, *SpringerBriefs in Business*. New York: Springer.

Carayannis, E. G., & Campbell, D. F. J. (2009). 'Mode 3' and 'quadruple helix': Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46* (3/4), 201–234.

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other. A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69.

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development*, *SpringerBriefs in Business* (Vol. 7). New York: Springer.

Chesterman, S. (2008). The turn to ethics: Disinvestment from multinational corporations for human rights violations-the case of Norway's sovereign wealth fund. *American University International Law Review, 23*, 577–615.

Chwieroth, J. M. (2014). Fashions and fads in finance: The political foundations of sovereign wealth fund creation. *International Studies Quarterly, 58*(4), 752–763.

Clark, G. L. (2009). Temptation and the virtues of long-term commitment: The governance of sovereign wealth fund investment. Working paper presented at the Asian Society of International Law, pp. 1–32.

Clark, G. L., & Monk, A. H. (2009). The legitimacy and governance of Norway's sovereign wealth fund: The ethics of global investment. Working paper. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1473973. Accessed 5 Mar 2015.

Cohen, B. J. (2009). Sovereign wealth funds and national security: The great tradeoff. *International Affairs, 4*, 713–731.

EsadeGeo Annual Report. (2014). Annual sovereign wealth fund report, EsadeGeo. Available: http://itemsweb.esade.edu/wi/Prensa/SWF2014_ENG.pdf. Accessed 04 Oct 2015.

Freedomhouse. (2015) Freedom in the world 2015 [Homepage]. Available: https://freedomhouse.org/report/freedom-world/freedom-world-2015. Accessed 07 Oct 2015.
Hacienda. (2016). Sovereign wealth funds, Hacienda, Chile [Homepage]. Available: http://www.hacienda.cl/english/sovereign-wealth-funds/economic-and-social-stabilization-fund.html. Accessed 14 Nov 2015.
Hufbauer, G. C., Wong, Y., & Sheth, K. (2006). *US-China trade disputes: Rising tide, rising stakes*. Washington, DC: Peterson Institute.
ISIF. (2015). Business areas. Ireland Strategic Investment Fund [Homepage]. Available: http://www.ntma.ie/business-areas/ireland-strategic-investment-fund/. Accessed 12 Dec 2015.
Khazanah. (2015). About Khazanah, corporate profile, Khazanah Nasional, Malaysia [Homepage]. Available: http://www.khazanah.com.my/About-Khazanah/Corporate-Profile. Accessed 11 Dec 2015.
Mauzy, D. K., & Milne, R. S. (2002). Singapore politics under the People's Action Party. Routledge London and NY.
Mubadala. (2015a). 'What we do', Mubadala, Abu Dhabi [Homepage]. Available: https://www.mubadala.com/en/what-we-do/defense-services/emirates-defence-industries-company#sthash.RKnzK46U.dpuf. Accessed 13 Dec 2015.
Mubadala. (2015b). 'Who we are', Mubadala, Abu Dhabi [Homepage]. Available: http://www.mubadala.com/en/who-we-are/overvipBIL.dpuf. Accessed 15 Dec 2015.
NBIM. (2015). 'Exclusion of companies', Norges Bank Investment Management [Homepage]. Available: http://www.nbim.no/en/responsibility/exclusion-of-companies/. Accessed 15 Dec 2015.
New Zealand Superannuation and Retirement Act (2001). Ministry of Social Development and the Treasury (Australia).
NZSF. (2015a). 'NZ super fund explained', New Zealand Superannuation Fund [Homepage]. Available: https://www.nzsuperfund.co.nz/nz-super-fund-explained/history. Accessed 16 Dec 2015.
NZSF. (2015b). 'Responsible investment', New Zealand Superannuation Fund [Homepage]. Available: https://www.nzsuperfund.co.nz/sites/default/files/documents-sys/Responsible%20Investment%20Framework.pdf. Accessed 17 Dec 2015.
Regjeringen. (2015a). 'Company exclusions, Norway Government [Homepage]. Available: https://www.regjeringen.no/en/topics/the-economy/the-government-pe/. Accessed 9 Oct 2015.
Regjeringen. (2015b). 'The government pension fund', Norway Government [Homepage]. Available: http://www.regjeringen.no/en/dep/fin/Selected-topics/the-government-pension-fund.html?id=1441. Accessed 8 Oct 2015.
Rose, P. (2008). Sovereign wealth fund investment in the shadow of regulation and politics. *Georgetown Journal of International Law, 40*, 1207.
Rozanov, A. (2005). Who holds the wealth of nations. *Central Banking Journal, 15*(4), 52–57.
Schena, P. J. (2012). The China Investment Corporation at 4 years: An evolving legacy of capitalization and control. *The Sovereign Wealth Fund Initiative*, 4–5.
SOFAZ. (2015a). 'About the fund', State Oil Fund Azerbaijan [Homepage]. Available: http://www.oilfund.az/index.php?page=bakikemeri&hl=e1.dpuf. Accessed 9 Oct 2015.
SOFAZ. (2015b). 'Content', State Oil Fund Azerbaijan [Homepage]. Available: http://www.oilfund.az/en/content/25. Accessed 13 Sept 2015.
Srinivasan, K. (2008). The macroeconomic implication of sovereign wealth funds. IMF working paper.
SWF Institute. (2015). 'Fund ranking', Sovereign Wealth Fund Institute. Available: http://www.swfinstitute.org/fund-rankings. Accessed 06 July 2015.
Thatcher, M., & Vlandas, T. (2016). Overseas state outsiders as new sources of patient capital: Government policies to welcome Sovereign Wealth Fund investment in France and Germany. *Socio-Economic Review, 14*(4), 647–668.
Thatcher, M. (2012). Western policies towards sovereign wealth fund equity investments: A comparison of the UK, the EU and the US. London School of Economics working paper.

Tranøy, B. S. (2010). Norway: The accidental role model. In X. Yi-chong & G. Bahgat (Eds.), *The political economy of sovereign wealth funds* (pp. 177–201). Palgrave Macmillan UK.

Truman, E. M. (2010). *Sovereign wealth funds: threat or salvation?* Peterson Institute.

Xavier, R. F., & Campbell, D. F. (2014). The effects of cyberdemocracy on the Middle East: Egypt and Iran. In *Cyber-development, cyber-democracy and cyber-defense* (pp. 147–173). New York: Springer.

Yeung, H. W. C. (2011). From national development to economic diplomacy? Governing Singapore's sovereign wealth funds. *The Pacific Review, 24*(5), 625–652.

Toward a European Cyber Public Sphere? 27

Matthias Galan

Contents

Abstract

Information and communication technologies (ICT) play a significant role in overcoming democratic deficits within the political framework of the European Union (EU). They are regarded as a tool to bridge the gap in representation and therefore increase input legitimacy. This chapter discusses examples of

Matthias is a freelance researcher and analyst in e-participation and online consultations as well as technology transfer in the renewable energy sector. Matthias holds a MA degree in political science and a BA degree in development studies.

M. Galan (✉)
Amsterdam, Netherlands

Vienna, Austria
e-mail: matthias.galan@gmail.com

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_10

e-participation and their potential for democratic innovation in the context of an evolving cyber-public sphere as prerequisite for the development of cyber-democracy. Against the backdrop of deliberative theory of democracy this chapter will focus on two European projects that have the potential to contribute to the creation of a cyber-public sphere and their democratic merit: the Open Consultation and the European Citizens' Initiative (ECI).

Keywords
Democratic innovation · European Union · ICT-based communication · Online consultation · European Citizens' initiative · Cyber-democracy

Introduction

The big efforts by EU institutions to engage citizens in debates about European politics via the cyberspace confirm the role ICT play as driving forces of social innovation. These new technologies emerge at a time when the relation between citizens, societies, and governments are in a process of fast-paced change. Eriksen explains that the model of the Westphalian state is put into question in a context in which the scope of social organization does no longer necessarily reflect its territorial boundaries. New forms of governance evolve above as well as below the state. The European Union, which has pooled sovereignty beyond the territory which it actually controls, might be the best example for this process (Eriksen 2009, p. 8).

Related to discussions about the scope of social organization are continuing public as well as academic debates on democratic legitimacy. According to Hurrelmann et al. three different positions can be distinguished. *One position* is asserting the erosion of the normative quality of democratic government. The main concern being that western societies are approaching a system of post-democracy, which is just a mere spectacle not able to claim a certain degree of value-based legitimacy. A *second position* understands current developments as the rise of a renewed interest in international and European politics, leading to a higher demand in democratic procedures to legitimate supra- and international politics. And finally, a *third position* is seeing no legitimacy deficit at all based on the assumption that nation states can successfully continue to carry out and regain responsibilities. (Hurrelmann et al. 2007, p. 2).

Debates about democratic legitimacy are often interrelated with how ICT influence individuals, groups, and society as a whole. They are often seen as a potential cure to the many issues related to democratic governance and legitimacy deficits. Especially in the context of the European Union, ICT is "a major tool in its communication policy in order to reduce the European 'information deficit', ensure transparency and acquire democratic legitimacy." Furthermore, these new technologies are considered as an efficient device for participatory governance, which is reflected in an "arsenal of online communication tools from institutional websites to webTVs and more, making use of most of the innovative online tools such as blogs,

Twitter, Facebook." As civil society organizations (CSO) gladly took on these new possibilities to communicate with EU institutions, one could already speak of a consensus on the usage of the Internet within the EU policy framework. This clearly contributes to the vision of a "cyber-pan-European democracy," while issues such as language and Internet literacy as well as communication with EU citizens remain. Therefore, the EU's engagement in ICT has to be understood as an ongoing process "alongside the evolving situation of internet equipment and culture" making a better understanding of "myth and reality of an EU cyber-democracy" necessary. (Carrara 2012, p. 356).

The emergence of a cyber-public sphere as essential part of a European cyber-democracy is put to the test when it comes to the influence that citizens can have on decision-making processes by using online tools. This chapter argues that while there are big efforts to use these tools to put information on EU politics out, the impact on decision-makers and policies is so far limited.

This chapter will look at participatory instruments within the EU framework based on a deliberative approach to democratic theory and discuss their potential for democratic innovation subsequently to the model introduced by Graham Smith (see Smith 2009). *First*, the complex relation of democratic legitimacy, deliberative democracy, and the cyberspace will be discussed. In a *second* step, current implications of a European public sphere and the normative turn toward participation of European citizens in decision-making processes will be scrutinized. In a *third* step, an analysis of two strongly ICT-based participatory instruments being online consultations (OC) and the European Citizens' Initiative (ECI) will follow. Finally, the innovative momentum of the two instruments will be compared in a *fourth* step based on the model of democratic innovation by Graham Smith (see Smith 2009).

Democratic Legitimacy, Deliberation, and the Cyberspace

This section will discuss the role the cyberspace plays in redefining democratic legitimacy. As Rodney Barker argues, the changes in political behavior today confirm that democratic legitimation is more than just voting. Therefore, it is necessary to look beyond elections and at the actions of citizens and their decisions. From this perspective a broad set of variables has to be taken into consideration, when looking at how citizens decide to participate or avoid the political system in general and European politics in particular (Barker 2007, p. 32).

Remarks on Democratic Legitimacy and Deliberative Democratic Theory

This chapter understands democratic legitimacy as being constituted by an input and output dimension, where input legitimacy is referring to participation in democratic procedures and output legitimacy to problem solving and control over the incumbents of power (Hurrelmann et al. 2007, p. 4). The dominance of output legitimacy

in EU politics has raised criticism that will be discussed in the following section. Elizabeth Monaghan argues that participatory elements of democracy were also neglected by democratic theory for a long time, because of doubts about the intentions of engaged citizens. Therefore, Democracy was rather seen as a way of choosing political elites than as a way to guarantee the direct rule of the people, as the works of Schumpeter or Dahl confirm. It is also due to mass movements in the first half of the twentieth century that participation as a way to secure democratic legitimacy was for a long time neglected (Monaghan 2012, p. 288).

In the light of changing voter behavior, it was deliberative and participatory democratic theory that gained a very prominent role in understanding this change. As Rainer Schmalz-Bruns explains, these approaches put emphasis on the procedural medium of a discursive decision-making process instead of a rather formalistic approach. The aim of the deliberative approach is to stand up to the claim to adapt democracy to processes of social and institutional change (Schmalz-Bruns 2009, p. 76).

To assess the quality of such deliberation, a public sphere as a discursive arena is crucial. Ideally, it is here where people can discuss questions of public interest in a sphere that is separated from the state and market and is reflecting the livelihoods of the participants. In an ideal case this arena would be characterized as enabling free, unrestricted, and rational communication. This shall allow individuals to question the actions of political actors as well as private actors in order to make sure that the latter are held accountable by the former. The underlying concept can be understood as a blue print for assessing legitimacy and efficiency of public opinion (Fraser 2009, p. 148).

In the terminology of Jürgen Habermas, the public sphere is a network of communication for opinions, where communication flows are concentrated into public opinions. The public sphere environment reproduces itself through communicative action, where a "natural" language is sufficient to understand a discourse. The public sphere constitutes a very complex network, which has different sometimes overlapping arenas. These are structured by thematic emphasis, policy area, and conflicting viewpoints (Habermas 1998, p. 436, 452).

This concept of a public sphere allows for the analysis of societal and European integration as it makes it possible to think the emergence of such a public sphere as the result of European communication networks. A major precondition being that a common political culture is put into existence, which is carried by a civil society (interest groups, NGOs, citizen initiatives, and movements). It is these actors of civil society who have to "conquer" arenas in which political parties reflect on decisions by the European institutions and accelerate the creation of European parties (Habermas 1997, p. 184).

This being said, the source for legitimation in deliberative democratic theory lies within the equal chance to state ones' interest in the process of decision making. By agreeing on and following the rules of the discourse, legitimacy is created. At the same time, this approach does distinguish itself from expert or elite-oriented approaches through the fundamentality of discursive rules instead of normative presumptions on power relations. In accordance, the communication running

through and constituting any given public sphere and its quality are of utmost importance. This is the case because legitimacy is derived from the way in which the deliberations are de facto organized and acceptable to its constituents. Communicative power has to be understood as societal power which is based on communication, being an open and collective formation of opinion. Only under these circumstances is a democratic public sphere possible (Möllers 2009, 259 ff).

Remarks on the Relation of ICT and Democratic Legitimacy

ICT can play a role in facilitating and strengthening participatory elements in democracy. At the same time, new technologies need to mature in order to avoid problems leading to lost trust in the political procedures and the political system as a whole. Keeping this in mind today's technology, and the increased interconnectedness of modern societies, hold a big potential for the innovation of democracy and therefore raise expectations for a renewal of democratic legitimacy.

With seemingly endless possibilities to use the right of freedom of speech, opportunities to exchange and challenge opinions, and to spread one's views, mobilization and participation might be seen as being easy to deliver through evolving technologies. But opinions of commentators on deliberative processes online and an emerging cyber-public sphere have been split. From an optimistic point of view this could lead to "participative, inclusive, and plural" decision-making processes. Other authors would rather see the participants engaging in these debates as already politically active, which would not at all increase participation. As computer mediated communication is rather "based on anonymity, absence of direct contact, and absence of moderation" some scholars doubt "the emergence of qualitative and accountable political debates". (Kies 2010, p. 3).

Related to the question if an actual increase of participation through online deliberation is likely, there are normative questions as well as technical challenges with implications for democratic legitimacy. According to Rogg, three points are of importance in this regard. *Firstly,* we have to consider that communication mitigated through information technology can increase transparency but at the same time can be used to hide important information. *Secondly*, we do have to bear in mind that there can be a misbalance between the increase of political processes and political communication being potentially considered and the number of people being able to actually consider this information. *Thirdly*, there is a certain selectivity regarding information to be made visible through new technologies and other information which is not reported at all (Rogg 2003, p. 77/78).

This raises the question on the relation between cyberspace and the public sphere and especially how it can be conceptualized. The further development of this relation is a process embedded in diverse and dynamic communication networks, where new ways of interaction are put to the test. At the same time, there are certain relevant groups and networks that are able to channel communication flows. Similar to other variants of public spheres – as constituted by mass media – there is not one coherent cyber-public sphere. As Dahlgren describes it, there are different groups who are on

the one hand through their "mushrooming" rather increasing fragmentation, sometimes leading to "cyber ghettos" while on the other hand rather traditional online party politics as well as e-government are centripetal forces (Dahlgren 2005, p. 152).

Today, ICT has changed the way in which we think about democracy – especially, if we consider the case of the EU. The cyberspace has to be taken seriously as another sphere of debates and deliberation, which – potentially – conveys democratic legitimacy to a political system. But the cyberspace is not an end in itself and needs to be understood as being interrelated with other democratic practices in the "offline world." Debates in a cyber-public sphere cannot replace other interactions of people, but ideally should enable people to develop their capabilities in understanding often complex topics, exchange opinions, and organize themselves.

The Case of the European Union

The European Union, as one of the major examples for new globalized social organisms beyond the Westphalian state, is recurring in its narrative on democratic principles and values. However, it falls short of adhering to these very principles itself – a paradox often referred to as the "democratic deficit." In the view of many scholars "(. . .) the EU can no longer be understood as an international organization whose legitimacy derives solely from member states but should be seen instead as a polity in its own right with direct links to its citizens" (Eriksen 2009, p. 2). The democratic deficit results in a legitimacy deficit as legitimacy today can only derive from democratic control.

But the urging question that remains is which democracy for which union? If the EU has left the status of international organizations, what status has it acquired? The definition debate has produced many different possibilities to describe the EU – transnational organization, a state in the making, a federal Europe, a Europe of regions, and many more. Reducing the complexity of the EU to only one of these ascriptions would be too narrow as it integrates transnational, supranational, and intergovernmental levels. This complexity is best expressed by the term "multi-level governance" which "encompasses intra-level and inter-level interaction of supranational, national and regional as well as territorial and functional actors all of which in addition to their official vertical and horizontal roles, tend to be part in a multi-dimensional policy network" (Karr 2006, p. 90).

Overcoming the Democratic Deficit

In this complex set up the EU is confronted with several alleged legitimacy deficits regarding structure (weak legislation, weak party system, etc.), process (cost and efficiency, lacking popular participation), and the project in itself (Eriksen 2009, p. 5). Which democratic model could fit such a complex structure and would do justice to democratic requirements on each of these levels? Many different models

have been developed that design democracy in relation to the perceived institutional set up of the EU. Common ground, except for maybe strict models of audit democracy that would see a legitimation process only guaranteed through the nation states and not through citizens, is deliberation. It is more or less common sense in democracy theory today, that "deliberation will increase legitimacy when affected parties are included and given a chance to argue their case" (Eriksen and Fossum 2012, p. 17).

In order to help us analyze the democratic deficit of the EU and the opportunities an evolving cyber-democracy brings, we can heuristically distinguish European democracy in institutional terms into *a polity* where authorized institutions make binding decisions as well as *a forum* that would be the communicative space in which every citizen should be able to engage, discuss, deliberate, and form opinions (Eriksen and Fossum 2012, p. 19). Of course, both institutional arenas are highly interdependent and interrelated. However, in the context of the EU, both show deep structural deficits that need to be addressed to (re)constitute democratic legitimacy. This chapter will rather focus on the realm of the *forum* which could also be referred to as the public sphere.

The EU polity is challenged on many levels when it comes to democratic norms: equality and representation are undermined by the overrepresentation of small states in the intergovernmental perspective and equality of voice beyond elections is a substitute to access to networks. The parliament remains the only institutional body of the EU that is directly accountable to and elected by the citizens while the council is often criticized for being too far removed from the citizens of the member states. Especially, the European Commission (EC) lacks democratic accountability and reflects the almost proverbial statement of intransparency and informality. Moreover, though the formal decision making power lies with the Parliament and the Council, it is the EC that initiates and drafts legislation in the first place. EU institutions themselves are often accused of lacking accountability, but in fact this accountability is also challenged by the missing intermediaries such as media and parties (Karr 2006, 96 ff.).

It is the *forum* or the public sphere in which incumbents are held accountable, where deliberation takes place and a *volonté general* is formed. As the EU is not only a union of states but also of citizens, European democracy requires a true European public sphere as the forum for its citizens. Such a European public sphere must be more than the addition of national public spheres when taking into regard, that the EU itself is also a supra- and transnational construct. Democratic legitimacy is always grounded on the collective will formed of the members of a specific political community, often referred to as the *demos*: "The demos, or the collective will of the people, is the founding myth and the telos of democracy" (Góra et al. 2012, p. 169). This paradoxon is inherent for processes of democratization. It turns the public sphere into a medium through which members of a community address themselves as a collective and are at the same time shaping their collective identity through common interaction and activity. In this sense, "collective identity is then no longer seen as a stable resource on which democracy can draw, but a shifting target that is contingent on democratic process" (ibid. Góra et al. 2012, p. 173).

However, in the case of the EU, we are facing a very fragmented and differentiated set of public spheres. The highly complex network of the public sphere has become as a result of globalization and new means of communication "polymorphus, polyphonic, and even anarchistic" (Eriksen 2009, p. 123). But in order to analyze the impact of changing means of communication on the public sphere, the term public sphere needs further operationalization. Far from being a homiletic block, it is more of a communicative network taking place on different, interdependent levels: a general overarching public, transnational segmented public (evolving around networks and actors with common interests and issues), and strong publics (institutionalized discourse among persons legally authorized to make collectively binding decisions) (Eriksen 2009, p. 130).

Regarding strong publics, they overlap significantly with the realm of polity. The only European institution that presents a strong public in the strict sense is the European Parliament, which is still not a fully fledged parliament, though the Lisbon treaty has brought several improvements.

An overarching general public sphere remains in the EU rather latent. Especially, language is seen as a main barrier to a community of communication. Though there are some European audio-visual spaces relying mainly on English as the new lingua franca, all in all the public communication remains scattered along language boundaries. This leads to a situation of missing intermediaries where parties and the media are organized in the national context and European topics play only a secondary role. (Karr 2006, 99 ff; Eriksen 2009, p. 133).

The transnational segmented publics are networks based on joint interests and are issue oriented. They can fluctuate, shrink, and expand depending on the momentum of their topic. These kinds of segmented publics are quite common especially in Brussels. However, their democratic value is ambiguous. In form of Civil Society Organizations (CSO), these networks can access formal and informal channels to EU institutions. But the effectiveness of their endeavors is strongly determined by their resources. Moreover, one has to bear in mind that these segmented publics are still a form of elite communication, where experts speak (mainly in English or French) to one another and lack themselves the democratic provisions of openness and equal access (Eriksen 2009, 133 f.; Karr 2006, p. 128).

Still these segmented publics and CSO, as one of their main actors, are seen as a transmission belt between the citizenry and the institutional level of policy making. Moreover, the action of CSO shall also help to develop a European identity where the demos is rather shaped through political means and civicness as a tool for the construction of identity (Eriksen 2009, p. 73; Freise 2008, 26 f.; Friedrich 2008, p. 71). This theory is based on the assumption that CSO across Europe would provide the same capacities and equally strong institutional settings. However, the tendency to speak of a European civil society is deeply flawed: "While there might be a more or less coherent 'Brussels civil society' made up of highly professionalized NGOs working in the EU capital, the assumption of homogeneity certainly does not hold when looking at the national level" (Finn 2008, p. 59). Especially, Eastern European CSO lack capacity and face, therefore, difficulties in placing their issues on the EU agenda (ibid. 2008, 55 f.).

Focusing on Participation: The EU's Normative Turn

Deliberative democracy offers alternative legitimization paths to democratize the EU beyond representational democracy given the weak input legitimacy of the EU due to the institutional setup – an opportunity that the EU is engaging for quite some time now. "(. . .) the EU has been geared toward reconnecting Europe with its citizens by building more effective policies, increasing transparency, and revisiting its communication policies" (Dalakiouridou et al. 2012, p. 298). Hence, civil society participation in the EU gained relevance since the transition from a primarily economic European Community to a more political European Union in the course of the Maastricht Treaty (Haidbreder 2012, p. 21, 27).

Though no direct notion of participatory governance can be found in the primary legislation of the EU up to the Treaty of Lisbon, the principles of proximity, representative democracy, and the rights of the citizens are anchored in the treaties before. The Treaty of Lisbon reinforces democratic equality, representative, and participatory democracy and gave birth to the first initiative of direct participatory democracy on the EU level: the European Citizen Initiative (ECI). But besides the ECI, no specific references are made to the realization of participation on a practical level (Dalakiouridou and Smith 2009, p. 5).

Regarding secondary legislation, "until 2000, the predominant view of democracy was implicitly connected to public access to documents (. . .)" (Dalakiouridou and Smith 2009, p. 5). The White Paper on European Governance (2001) represents a turning point as it labels openness, participation, accountability, effectiveness, and coherence as the five principles of good governance (European Commission 2001, p. 10) and thus gives way to the voluntary inclusion of civil society. The White Paper proved, however, to be less ambitious regarding concrete reforms as it did not challenge the decision-making process in place. Still it inaugurated the third generation of a consultation regime – moving from the terminology of "partnership" in the 1960s/1970s to "consultation" in the 1980s/1990s finally to "participation" (Haidbreder 2012, p. 15). The most important follow-up tool was the Interactive Policy Making platform that got the focal point online consultation at EU level (Dalakiouridou and Smith 2009, p. 5).

Communicating Europe: e-Participation and the EU

In 2005, the Commission adopted the Plan D for Democracy, Dialogue, and Debate (revised in 2006) that shall support bottom-up civic initiatives and is together with the action plan to improve "Communicating Europe" seen as the adoption of a new "listening attitude" (ibid. Smith 2009, 5 f.). E-Participation is becoming more and more important as a means to reconnect Europe to its citizens: "(. . .) the EU seems to have employed 'legitimacy-enhancing deliberation' logic, whereby the institutional eParticipation offerings reinforce deliberation among participants but without bestowing direct authority" (Dalakiouridou et al. 2012, p. 308). The result is an extensive list of e-participation initiatives by the EU (most are, however, already

closed again) and a long list of social media channels through which EU institutions seek the more active involvement of the citizens (see ibid. 308 ff, p. 315).

"In summary from 2000 onwards, the documents adopted by the Commission relate to transparency and accountability, while from 2002, consultations are given more prominence as a citizen contribution to the policy making cycle" (Dalakiouridou and Smith 2009, p. 6). E-participation is integrated in the EUs Digital Agenda (https://ec.europa.eu/digital-agenda/en/eparticipation). Here, the European Commission defines it as an important way to help people engage in politics and policy-making and make the decision-making processes more understandable. A European eGovernment Action (https://ec.europa.eu/digital-agenda/en/european-egovernment-action-plan-2011-2015) Plan is in place that shall help to better coordinate national and European policy instruments and support the transition to eGovernment platforms. Furthermore, the website "your voice in Europe" (http://ec.europa.eu/yourvoice/index_en.htm) was established to serve as the "single access point" to e-participation opportunities. It links online consultation processes, blogs, and social media channels and seeks to enable the citizens to play an active role. The most established tool is the EC online consultation that is on this page also the most active tool. Curiously, the ECI is only mentioned in the "useful links" section, even though this initiative is also strongly reliant on ICT.

Assessing the Potential for Democratic Innovation

New initiatives in the realm of democracy are not necessarily innovative. Simply because e-participation is a relatively new tool, it does not mean that there is value added in terms of democratic legitimation. We will now turn to the analysis of implications on how the assumed increase in legitimacy through participatory instruments based on ICT is in a way leading to democratic innovation, which might be contributing to a cyber-democracy, a clear precondition being a cyber-public sphere capable of allowing for stronger involvement of citizens in democratic procedures.

The model applied in this chapter, in order to assess the democratic innovation and increase of democratic legitimacy through participatory tools, is based on the work of Graham Smith, who is bringing together direct and deliberative approaches to democracy in an analytical framework (Smith 2009, p. 11). In this analytical framework, the emphasis is put on four democratic goods, "namely inclusiveness, popular control, considered judgement and transparency" (Smith 2009, p. 12). These four goods are indispensable to an understanding of democratic legitimacy, even if the way in which each of those goods is emphasized in single theoretical approaches might be differing. In addition, and to put these four rather theoretical terms into a practical context of democratic innovation, an understanding of efficiency and transferability needs to be included into the equation. While efficiency gives us an idea about the "costs that participation can place on both citizens and public authorities," it is transferability that "provides an occasion to evaluate whether

designs can operate in different political contexts, understood in relation to scale, political system or type of issue" (Smith 2009, p. 13).

This "matrix" allows for a close assessment of how innovative ICT-based deliberation and democratic instruments employed in the EU really are. Only an increase in these variables through new democratic initiatives can lead to the assertion that they represent a real democratic merit. Additionally, we will address the question of an emerging European public sphere, as this is one of the most important issues of innovating European democracy. We will now take a closer look at the implications and operationalization of the single democratic goods as well as effectiveness and transferability.

The main questions of **inclusiveness and equality** are *who is actually to be included* (depending on the applied concept of citizenship) and *which selection mechanism* is in place: "institutions can operate a variety of selection mechanisms, from designs that are open to all, to those that restrict participation through mechanisms such as election, random selection and appointment" (Smith 2009, p. 21). Moreover, one has to ask *how to guarantee equality* of diverse groups and people in order that they can have the same possibilities and means to influence a decision-making process.

As Smith concludes on this point, there is a need for attention to the ways in which "institutions encourage different types of contribution and offer support and resources to those citizens who have little experience and/or are intimidated by the thought of speaking in public" (Smith 2009, p. 22).

Popular control puts emphasis on the extent to which citizens are able to control political processes. In most decision-making processes there is no total popular control, it is rather at predefined stages that there is a say for citizens. An innovative approach would have to focus on the efforts of decision-makers to actually guarantee that there is sufficient space to enable that citizens can have control of decisions taken in their name. Therefore in accordance to Smith, we have to consider "all four stages of the decision-making process" being "problem definition, option analysis, option selection and implementation," and we have to be "aware that the design of democratic innovations may involve citizens in 'sharing' power with other actors" (Smith 2009, 22 ff.).

Considered judgment focus on possibilities for citizens to consider, deliberate, and decide on given political issues. This is a central point to the legitimacy of citizen participation in decision-making processes. But this is not only related to an understanding of "technical" facts but also to an understanding and acceptance of other opinions by people with often widely differing social perspectives (Smith 2009, 24 ff.).

According to Smith, there are two ways in which **transparency** becomes a "crucial consideration." The involved citizens need to have a clear understanding of the conditions "under which they are participating, which are related to the selection process of the issue at hand or who is organising the process as well as the potential outputs and their influence on the political process." A *second* precondition in this respect refers to the transparency of the process not only to the involved participants but also to a wider public. This external transparency can be seen as

publicity, describing the "transmission of information about the institution and its decisions to the wider public" (Smith 2009, p. 25). The strategies organizers pursue in this respect can differ from rather passive stand points where only "publishing documentation through official sources" is taking place to an active promotion and media (Smith 2009, p. 26).

Smith understands **efficiency** as in relation to the "costs" of involving or not involving citizens in political processes. While he sees many theorists and practitioners claiming that participation is per se a "virtue" holding many benefits, he continues to argue that we also "need to consider the demands they place on citizens and on other institutions and whether these are worth bearing individually and socially" (Smith 2009, p. 26).

Transferability is meant to challenge the criticism on the transferability of participatory practices. In this approach, a lot of importance is attributed to the way in which the designs of such processes with a high degree of participation of citizens can be put into another context of decision-making and under what preconditions this is a promising enterprise. (Smith 2009, 26 ff.)

Case Studies: Online Consultation and ECI Compared

The case studies chosen cannot reflect the diversity and wide range of online participation tools used in the EU (see Dalakiouridou et al. 2012, 308 ff.). However, they are the two most significant examples as the online consultation is the most established tool and the ECI is expected to take e-participation in the EU to a new level. Moreover, the examples chosen represent different generations of participation regimes in the EU – ranging literally from consultation to direct participation. By comparing these two different democratic approaches, yet staying in the theoretical realm of deliberation, we can scrutinize their level of innovation and eventually contribution to enhanced democratic legitimacy in the EU. While the ECI is designed to address an overarching European public sphere, the online consultation is based on the idea of networks and segmented public spheres. However, both shall contribute to enhanced democratic legitimation through communication.

One factor that is affecting both initiatives equally is the access to the Internet across the EU as all forms of cyber-democracy must rely on stable Internet connections – be it on mobile devices or on a desktop PC. A Eurostat survey from 2012 shows that on average 73% of the EU population is using the Internet any place. However, if taking a closer look at the realities of the different member states in 2012, it becomes clear that there is a digital divide yawning between North and South (e.g., Sweden 93% as opposed to 57% in Italy) and West and East (Germany 82%; Romania 48%). Only 50% of Romanian households had broadband Internet access in 2012. However, the number of broadband connections to households almost doubled from 2010 then lingering at a mere 23%. The number of people using the Internet at any place rose to 78% in 2014 showing that since 2012 a considerable number of Europeans gained access to the Internet. But

statistical data shows that the digital divide in Europe remains significant. Still, there are some countries with a considerable number of people who have no Internet access at all. This includes Romania (39%), Bulgaria (37%), Greece (33%), Italy (32%), and Portugal (30%) and gives proof to the persistent divide between North and South as well as East and West (Seybert 2012, 1 f.; Seybert and Reinecke 2014, 1 f.).

Though general access to Internet and broadband connection is taking up speed, we cannot neglect that the lack of access to the Internet is a major barrier for online participation. Especially, Eastern European countries are easily excluded from participatory processes violating the principle of inclusiveness massively. Thus, when discussing e-participation initiatives we must keep in mind that access to Internet is far from perfect and that the digital divide will prevail for some more years to come. Against this background, we will scrutinize the impact the tools can have in this imperfect environment for democratic legitimization. The following analysis is based on a literature review and on expert interviews.

The European Commission's Online Consultation Tool

Online consultations are the consultations that are announced on the Internet (see homepage "your voice in Europe" on "Europa portal") and which can be answered using different electronic means as online questionnaires or email. Information on the issue (e.g., consultation documents) is also available online. OC are so far the main mean of citizen involvement with sometimes more than 100 OCs taking place per year. Their use, however, varies widely across directorate generals (DGs) and they are a voluntary tool of the EC (Quittkat 2011, 658 ff.; Dalakiouridou et al. 2012, p. 316).

Upon the announcement of an OC on the web portal, different target groups can give their opinions. In the "open" target group all actors and interested parties are welcome to participate. Selective OC generally address well-defined groups on rather technical issues while closed OC are limited to business/business organizations, public authorities, or both. The format of a consultation process ranges from standardized (closed questionnaire), semistandardized (questionnaire with open questions), and nonstandardized (text can be freely commented). Consultation is open for a minimum of 2 months and after evaluation EC should publicly report on the inputs and their evaluation. OC can take generally place at any stage of policy making. In general, they tend to be used the most in the initial phase of the cycle (Quittkat 2011, p. 653, 660 ff.).

The OC are expected to increase the democratic legitimation of the EU. Being in place for over a decade now, empirical and scientific data on the results have been collected and evaluated (see Quittkat 2011; Rasmussen and Toshkov 2013). Against the backdrop of the operationalization of deliberation of Smith, this chapter will scrutinize whether the OC have led to improved inclusiveness, transparency, public control, and considered judgment. Issues of efficiency and transferability will also be discussed as well as the notion of a European public sphere.

Inclusiveness

New access channels like the OC generally lead to an increased openness to organizations and interest groups. The introduction of new media in the consultation process is a shift from the narrow concentration on Brussels-based CSO to a wider public beyond territorial limitations which can be seen as a massive change in access to the EU policy-making process. Most of the OC (90.37%) are addressing open target groups, i.e., are accessible to everyone who is taking interest in the topic. Only a minority of OC are either selective (6.04%) or closed (3.59%), proving at least formal access and inclusion to all interested groups in the vast majority of OC (Quittkat 2011, p. 660; Haidbreder 2012, p. 16; Karr 2006, p. 128).

However, scientific research shows that not all actors are equally included in the process. Foremost, the North–South and West–East divide also applies to OC. New member countries are much more reluctant to participate and also members from Southern Europe are underrepresented in relation to their population. Moreover, "(. . .) while there exists an equal chance of access to OC for organized civil society, our data disclose considerable inequality among the interest positions represented" (Quittkat 2011, p. 667). Often business and business interest associations make up 39% of all participants in OC. The numerical importance of this single largest group challenges the principle of equal inclusion. Participation in OC is very resource consuming in terms of work force and time. Ironically, as consultation is more open business seems to benefit more from OC as they can invest more resources than CSO or individuals (ibid 2012, 667 ff.). With this information one can easily argue that the thin line between "consultation" and "lobbying" gets rather blurred.

Moreover, as mentioned before no natural equilibrium exists between CSO themselves. Due to the high demands for expertise and resources to effectively participate in OC, it is very organized, highly professionalized, and Brussels-based groups who remain the standard representatives of CSO. "Until now, the preexisting territorial and resource dependant bias that privilege certain CSOs over other less organized, professionalized and more locally anchored civil society seem to persist also in online consultation system" (Haidbreder 2012, p. 16). To foster equal inclusion, the EU funds CSO and thus helps them to acquire necessary expertise and resources. However, EU funding is always driven by its own policy goals reflected in the EU budget and can hence not necessarily lead to a development of critical and independent CSO arena (Friedrich 2008, p. 78).

Popular Control

"For the time being, the participation of civil society organization has to be characterized as 'participation by grace and favor'" (Friedrich 2008, p. 78). OC are no exception as it is only implemented on a voluntary basis, depending on the will of individual civil servants and differ, thus, in their form and impact widely across the different DGs, policy fields, and levels (Haidbreder 2012, p. 16). Moreover, OC are mainly used (about two thirds) in early phases of the policy cycle at the stage of policy formulation. While this is an important step in the cycle, it is far from the step where actual binding decisions are made. The EU perceives the tool of OC more as a means of problem solving and that seeks input from experts rather than actual

decision-making authority (Dalakiouridou and Smith 2009, p. 3; Haidbreder 2012, p. 16). "The more concrete the facts of a case, the less the Commission is prone to consult the wider public" (Quittkat 2011, p. 660).

And also, the format restricts real popular control over decision-making as many of the OC are using the semistandardized or standardized design rendering consultation sometimes into mere box ticking exercises that leave less room for genuine innovative input. Quittkat comes to the conclusion that the EC is "emphasizing participation (quantity) at the expense of input (quality)" as the more open the format the lower the overall number of participants (Quittkat 2011, p. 662).

Overall, the OC have clearly not been designed to put real public control into the hands of CSO or citizens and proves to be hardly innovative in this very field.

Transparency

The OC have increased transparency to a certain degree, as they give online access to information and channels consultation to more formal channels, but "whether, in which way, and to which degree the Commission incorporates inputs from various consultation procedures is fully up to the Commission's undisclosed appraisals" (Haidbreder 2012, p. 16). Especially, the reporting part on consultation shows weaknesses as only one third of the OC also provide reports on the consultation or make contributions from other participants accessible on the web. And even if there is a report available, it remains unclear which process of input assessment was adopted, i.e., which criteria were used to evaluate different contributions. Often the reports that are available give proof of the insufficient input assessment criteria: "They miss out arguments; overstate the standpoint of 'big' EU-level associations, the social partners and EU member states; and fully ignore contributions from private persons and give only little room to representatives of general interest associations (. . .)" (Quittkat 2011, p. 664).

Regarding transparency, especially the use of modern communication technologies would put the European Commission into a position in which it could easily improve transparency of the OC. However, up to date, it fails to do so and can thus not contribute to enhanced democratic legitimation due to a continued significant lack of transparency.

Considered Judgment

With contributions not being made accessible and no forum for exchange offered, considered judgment is hardly to be expected as it depends on two-way communication. As expertise is necessary for participation, one can assume that there is an understanding for technical details of contributors. However, other positions in the "debate" are not disclosed and discussed.

The only form of considered judgment can thus be found in the responsiveness of the EC, i.e., if after the consultations traces of the arguments CSO have put forward can be found in the policy drafts. Friedrich has analyzed two policy-making processes and both of them revealed that although CSO had the opportunity to get heard, little consideration of their concerns was finally made (Friedrich 2008, 78 ff.).

To facilitate considered judgment transparency would be a prerequisite. To design consultation more in a form of real dialogue additional web-based tools like online discussions or webinars could be offered in accordance to OC. Again, EC stays behind its possibilities and is hardly establishing innovative participation tools, if they fail one of the main characteristics of deliberation.

Efficiency and Transferability

The adoption of OC lowers the cost of information dissemination and feedback collection. Especially, standardized questionnaires render OC a very effective tool although efficiency is not necessarily given if quantity is emphasized at the expense of quality (see above).

One of the main advantages of the OC could be that it is easily transferable in ways of policy fields and also EU institutions. The Council or the Parliament could theoretically adopt OC and simply use the software of the EC.

European Public Sphere

The idea of CSO as transmission belts between EU citizens and institutions rests on a model where CSO pick up the concerns of citizens, voice them to a wider public to discuss issues and then carry them to the institutions – also referred to as agenda setting. However, this function as a transmission belt is hardly given in the case of OC as the agenda is set by EC initiative. OC take place in highly segmented public spheres in which only those actors with an interest in the topic engage. The current structure of OC, where high resource input is a prerequisite for efficient contribution, favors contacts with Brussels-based associations. "This specific structure of European civil society explains, among other things, why EU-level NGOs appear regularly too elitist and hence fail to assume a Europeanizing function as conceptualized by advocates of active citizenship" (Haidbreder 2012, p. 26). Those segmented publics are highly differentiated and organized around problem-solving turning the public discourse issue oriented and "rendering its putative democratic merit an unintended by-product" (Eriksen 2009, p. 150).

The OC cannot make up for the missing link between citizens and institutions. Regarding a European public sphere, it is only contributing to segmented public spheres – often restricted to the "Brussels bubble." "However, the plethora of transnational deliberative publics that mutually observe each other have normative value in themselves. They do not suffice to constitute a democratic sovereign, but public deliberation generally increases information levels, reduces the problem of bounded rationality, and forces participants to justify their claims" (Eriksen 2009, p. 150) – even if only to a limited extent as in the case of the OC.

The European Citizens' Initiative

The formal introduction of the ECI in 2012 as a tool to voice concerns of citizens toward the EU institutions was welcomed with a lot of optimism by CSOs. According to article 11(4) of the Treaty on European Union, it allows "not less

than one million citizens who are nationals of a significant number of Member States [to] take the initiative of inviting the European Commission, within the framework of its powers, to submit any appropriate proposal on matters where citizens consider that a legal act of the Union is required for the purpose of implementing the Treaties." Its introduction was seen as a considerable milestone in a process that was in the making since the 1990s. But the phase of optimism after the introduction of the ECI was short-lived as organizers experienced many difficulties with setting up an ECI and frustrations with the outcome of successful initiatives. A report by the Committee of Constitutional Affairs in the European Parliament criticized that "only 3 out of 31 registered ECIs have reached the final stage" of an answer by the European Commission (EP 2015, p. 8).

After three years, the first round of evaluation of the ECI Took place. In late 2015, the European Parliament adopted a resolution based on a report by the Committee of Constitutional Affairs. This report criticizes the "dramatic decrease in the number of new initiatives" as a consequence of "disproportionate requirements and of an unnecessarily complex system." Furthermore, it goes on to express regret "about the lack of legislative impact and the discouraging follow-up by the Commission of successful initiatives." In this resolution, the EP asks the EU institutions and member states to take all necessary steps to promote the ECI and to foster citizens' confidence in this tool. One of the suggested measures is to provide funding to organizers of ECIs, which shall include promotion on TV and radio. (EP 2015, 8 ff.)

Opinions do widely differ, especially, in the question of how far EU institutions have to react to a successful ECI and how the further process should look like. While the EP wants a stronger ECI, the EC is more hesitant. It states in its report on the implementation of the ECI that one of the main benefits is to facilitate Pan-European debate. The question in how far this has to be considered by the EC and followed up by concrete initiatives remains open. (EC 2015, p. 2).

The ECI resembles a referendum, where signatures can be either collected online or offline and have to meet certain standards that depend on national regulation. Regulation 211/2011 establishing the ECI is the result of a long and contested process to establish a citizens' initiative at the European level. Central questions in the discussions were how the threshold of signatures from the qualifying member states should be defined, citizenship as a requirement to take part, and the age of signatories. The biggest disputes focused on the collection of ID numbers, because it is required in some member states to verify a signature (Monaghan 2012, 292 ff.).

The role that ICT has played in organizing ECIs has always been significant. Carrara explains that of at the time "10 ECIs, the internet has been used as an additional (6/10) or as an exclusive (4/10) means of transnational campaigning and collecting signatures" (Carrara 2012, p. 356). This was a pioneering act keeping in mind some "degree of prediction of the provisions of the final Regulation" (ibid.). But "e-ECIs" have to be seen as a "new step in attempts to build a cyber-pan--European democracy" (ibid., p. 366). A report by the European Commission evaluating the first three years of the ECI states that of the collected statements of support "around 55% [. . .] were collected online" (EC 2015, p. 7).

There are several general requirements (It has to be noted that the European Parliament has asked the EC and member states to harmonize the requirements across Europe (see EP 2015)) that have to be met by organizers and by signatories. First of all, the ECI can only be organized and endorsed by European citizens, who are allowed to vote in elections to the European Parliament (Szeligowska and Mincheva 2012, p. 276). Secondly, the initiative should not "manifestly fall outside the scope of the Commission's power of legislative initiative under the treaties" be not "manifestly abusive, frivolous or vexatious" and not be "manifestly contrary to the values of the Union as set out in article 2 TEU" (ibid., p. 277/278). Thirdly, it has to meet formal requirements such as information on the initiative and its purpose as well as continued updates (ibid., p. 278). A fourth requirement is that a citizens' initiative needs "to be signed by at least one million citizens" (ibid.). A fifth point is the territorial element, where signatures need to "have come from at least one quarter of Member States" and meeting a "minimum threshold of signatures to be met, which is established by multiplying the number of MEPs of the Member States concerned by a factor of 750." An initiative needs to collect this minimum number of declarations of support in at least seven member states. Finally, the organizers are responsible for the collection of statements of support by "using specific forms provided for in the regulation" (ibid.). Greenwood criticizes that these requirements create a lot of administrative and technical costs for the organizers (Greenwood 2012, p. 330).

The first three years of the ECI show that it still needs to find its place within the framework of European politics. While it offers a unique way for civil society to give its demands a voice, it remains to be seen in how far it will be a tool to translate demands by campaigners and their supporters into legislative initiatives. On the following pages the innovative momentum of this tool will be analyzed.

Inclusiveness

In regulation 211/2011 establishing the ECI, it is clearly stated that this instrument is open to all European citizens allowed to vote in EP elections. In theory, this makes the ECI an instrument including all citizens of the European Union. But this clearly inclusive aim to give European citizens a voice is contrasted by several selection mechanisms decreasing inclusiveness and equality of the instrument. One of the central aspects of inclusiveness is access, on the one hand to relevant information on the issues which the ECI wants to have solved and on the other hand to how it works. This requires organizers and supporters to have significant organizational capabilities including ICT skills. As Garcia and Del Rio Villar argue, the ECI is another mechanism that might be used to contribute in the policy-making process by enabling citizens and their organizations to "introduce legislative proposals" (Garcia and Del Río Villar 2012, p. 316). This would make them co-owners of the policy-making process and therefore strengthen "the link between the EU political arena and the public sphere" (ibid.). Critics on the other side claim that current participation is elitist and constituted by already organized lobbying groups and organizations, which use the ECI to gain influence (Monaghan 2012, p. 290). Language does also constitute a relevant selection mechanism – citizens willing to engage in an ECI

would require on the one hand to be able to speak English and on the other to be able to use the Internet (Carrara 2012, p. 356).

An important feature to safeguard equality would be to keep the collection of signatures as user-friendly as possible and at the same time make sure that online procedures are secure. The challenge in this regard is that organizers and the verifying member states need to make sure that signatories are real persons and their signatures can be counted as genuine (Carrara 2012, p. 363). Regarding the collection process of statements of support, there are controversies because of differing requirements demanded by member states as some require ID numbers to verify signatures while others do not (Monaghan 2012, p. 294).

The ECI has the potential to include more citizens in European decision-making processes. But during the last three years, there has been a lot of criticism on the lack of clear rules for organizers and participants. The confusion about these very complex rules makes it harder to include citizens in the process. Therefore, it is efforts to reform the tool that might make it a truly inclusive instrument in the future. Potentially, it allows for a wider discussion of EU policies led by CSO which have the necessary resources to organize campaigns. When it comes to organizing an ECI and campaigning, success is based on a strong engagement by organized interest. Inclusion will depend on the evolving interplay of citizens, CSO, and the institutions in voicing common concerns and a clear framework for further debate and action.

Transparency

Transparency is to a certain extent assured by publishing relevant documents and information on EU websites, which is a minimum standard (Smith 2009, p. 25). There is support for citizens and organizers who either want to get information or start a new ECI as well as some publicity through events organized by the Commission. Therefore, conditions for participation are to a certain degree transparent. Nevertheless, there is a lot of criticism by organizers. This has several reasons. For many organizers, the decision, if an initiative is rejected, is taken in an intransparent way as it is unclear how decisions are taken by the EC. The rules for organizing an ECI are complex and vary from member state to member state, making the process for organizers unnecessarily confusing. Furthermore, there needs to be overall improvement regarding what happens after an ECI was successful, for instance, when it comes to adopting legislation based on an ECI. CSO see it as harmful to the transparency of an ECI that the Commission is involved both in the beginning and the end of an ECI. This puts a lot of influence on the fate of an initiative in the hands of one institution.

Popular Control

The ECI as a participatory tool is meant to enable public control of shaping policies to a certain extent. There are possibilities of taking control during the registration procedure of the ECI foreseen in the regulation. According to article 4 paragraph 2 and 3, the Commission is obliged to carefully examine every registration and if rejected has to give a statement on the reasons for rejection as well as information on judicial and extrajudicial remedies (EC 2011). Citizens therefore

and in accordance with article 10 of the regulation have the possibility for a "democratic audit" as the Commission has to respond to and meet the initiators of ECIs as well as give a "precise feedback on its final decisions" (Garcia and Del Río Villar 2012, p. 315).

Nevertheless, the question if there should be deeper accountability of the Commission and the institutions is not yet solved. Overall, the organizers of seven ECIs have taken the European Commission to the European Court of Justice (ECJ). The first initiative to take this step was "One million signatures for 'a Europe of solidarity'." The goal of the initiative was to ask the EC to put forward legislation "to enshrine in EU legislation the Principle of the 'state of necessity' [whereby] [w]hen the financial and the political existence of a State is in danger because of the serving of the abhorrent debt the refusal of its payment is necessary and justifiable." The EC rejected it because it thought it to fall manifestly outside the framework of its powers. In September 2015, the General Court of the ECJ confirmed this decision and argued that the initiative "does not have any basis in the Treaties" (ECJ 2015).

Overall popular control is quite weak as of the four stages of decision-making only during the first two stages of problem definition and option analysis there is a possibility to take control of the content. Even if an ECI is successful, discussion of the content in the EU legislative bodies (the Parliament and Council) is not guaranteed (Garcia and Del Río Villar 2012, p. 316). If compared to other popular referendums, the ECI therefore might have less impact on decision-making processes. The nonbinding nature of the ECI leaves its political significance to the willingness of the Commission and the legislative bodies to accept reasonable political demands by the citizens (Cuesta-López 2012, p. 267). Nevertheless, the possibility for citizens to "formally participate in the EU decision-making process" by presenting their initiative to the institutions can be considered as "a significant evolution for the EU political system" (Garcia and Del Río Villar 2012, p. 319).

Considered Judgment

As evidence from the ECI shows, enabling citizens to come to a considered judgment is a challenging task not only for the institutions but also for organizers. A significant part of dissemination on the ECI is done through "websites and social media/networks such as Facebook, Twitter, etc" (Carrara 2012, p. 358). Already in this information stage of piloting, ECIs' most organizers did avoid to open multilingual online forums for the costs would have been too high, which shows that language as well as Internet literacy are crucial questions for considered judgment (ibid., p. 357). There are further limitations in developing online strategies, when the ECI enters the phase of convincing people and collecting signatures as "the level of multilingualism of the central collection website (in most cases a dedicated website rather than special pages of an existing one) is essential to make it accessible to as many European citizens as possible" (ibid., p. 358). This shows that linguistic resources are crucial to allow for citizens to come to a considered judgment. Language therefore is still a "strong limitation to citizens' discussion and deliberation in the process of ECIs" (ibid., p. 357).

One remedy to this problem would be a truly pan-European media landscape to enable citizens to get information on political issues (Carrara 2012, p. 356). So far, experiences such as Euronews have shown that this remains limited to some political and economic elites (ibid.). This makes it necessary for civil society networks supporting ECI committees to "make an extraordinary effort in order to raise political debate beyond domestic affairs and to manage the transnational gathering campaigns" (Cuesta-López 2012, p. 267). Even if the current situation makes it quite hard to spread information on ECIs, there is still a potential for this instrument to become a means of "pan-European mobilisation and communication" (Garcia and Del Río Villar 2012, p. 320). As Garcia and Del Rio Villar observe the campaign to promote the ECI is already, to some extent, an example how the ECI "could contribute to pan-European deliberation as organisations establish a dialogue and discuss common objectives" (ibid.).

Efficiency

The literature and interviews show that the cost of involving citizens and generating input legitimacy through this instrument remains unclear. Furthermore, EU institutions remain hesitant on obligatory follow-up processes to an initiative. While organizers and the European Parliament want to see a stronger participatory element, the EC primarily sees it as a means of spurring debates in Europe. Because of these differing opinions on the degree of participation, it remains unclear if there will be a bigger role of the ECI in putting forward legislation. In addition, there has been a lot of criticism on the organization of ECIs. Efficiency of procedures and clear outcomes are therefore crucial for the ECI to be taken seriously by citizens. Persistent issues with registration and online platforms show that it needs a strong commitment and the necessary resources to guarantee the efficiency of the procedures from the start to the implementation of potential regulations or directives based on an ECI. Regarding the costs and benefits there are not only material but also "organisational and political" considerations which have to be kept in mind. Finally, the "main cost consists in gathering one million signatures in a quarter of the Member States" (Garcia and Del Río Villar 2012, p. 318). Overall, as the EU is mostly dominated by an output-based approach, "success of the ECI will be measured in terms of how many initiatives lead to a Commission Green Paper or Proposal for a Regulation" (Monaghan 2012, p. 296).

Transferability

Elizabeth Monaghan argues that transferability will be depending on the successful implementation of the ECI (Monaghan 2012, p. 296). Some EU member states such as Germany or Austria have comparable instruments while others do not know this kind of tool. The ECI could, in this regard, pave the way to make it easier to transfer such an instrument to other levels of governance. This will depend on the experience with this instrument on the European level. From a technical perspective, minimum standards allowing citizens to easily understand and act in accordance with regulations will be important. Furthermore, transferability of the platform used to conduct an ECI could be a blue print for other levels of governance. This could be

encouraged by making it open-source to allow developers to further work on democratic tools that can feed into the existing platform.

Way Toward a European Public Sphere and Cyber-Democracy

In comparison to other participatory instruments within the EU framework, e.g., the civil dialogue, benefits for supporters to an ECI might be rather small when compared to the necessary effort of organizing such an initiative, which is why it will depend on the Commission and also the other EU Institutions to take the outcome of ECIs seriously (Garcia and Del Río Villar 2012, p. 318). The question arises if the costs related to preconditions and compliance with procedures in comparison to the potential outcome might not be too high for organizers, while one million signatures might be easy to dismiss in comparison to the overall EU population (ibid., p. 319).

The ECI certainly increases discussions on topics related to the EU, but the question still remains, who will be willing and able to mobilize a wider public to rally for a common cause. As initiatives since the early 2000s have shown, there is quite a lot of failure to "mobilise a wider public" by civil society organizations, which "leaves room for doubt about the capacity of an instrument such as the ECI to foster broader public participation and thereby redress concerns about a democratic deficit in EU decision-making" (De Clerck-Sachsse 2012, p. 307). Therefore, a closer examination of problems with the mobilization of the public for EU policy issues would be necessary (ibid.). Evidence of the first successful ECI contradicts this to a certain extent. Of the three successful initiatives all were relying on strong organizational support by CSO such as trade unions or the church. As they act in the interest of their peers the question still remains to which extent issues from "the grass root" can attract enough support to make it through the process.

Synthesis

When evaluating e-participation tools adopted by the EU, one has to keep in mind to analyze them in the according environment. They are embedded in a certain social context, e.g., the North–South and East–West divide when it comes to access to the Internet or the level of professionalism of CSO. A cyber-public sphere is by no means to be seen as parallel to the existing realities – it is not a second world but brings the possibility to enhance communication. But barriers that prevail in the analogue world, like language barriers, are also prevailing in the digital world. Therefore, as any other democratic innovation, e-participation has to struggle with societal givens and must try in its design to overcome those.

Regarding inclusiveness and equality, the OC certainly was an improvement when introduced almost a decade ago. However, the practical use of the OC reveals several problems in terms of equality and inclusiveness. The ECI has still to stand up to the high expectations, especially, when talking about inclusiveness and equal access. Clear rules and procedures will be crucial to accomplish this task. Critics do fear that the ECI as an instrument is already being hijacked by Brussels-based and

well-organized national CSO, rendering it into a tool of "elite" interests instead of genuinely including the opinions of EU citizens.

Transparency certainly is the Achilles Heel of the OC. Though it might contribute to transparency by revealing to what kind of policy formulation the EC is up to, however, the consultation process itself is absolutely in transparent. The ECI is at least designed to fulfill minimum criteria for transparency during the process. However, the decision taken by the EC to register an ECI and the question what happens after a successful ECI remains intransparent. It is also seen as detrimental to transparency that the EC has such a strong position in deciding about the fate of an initiative and is at the same time in charge of further legislative action. Steps for further action are not clearly defined and need further improvement by the European institutions.

While the OC are clearly not designed to put decision-making authority into the hands of CSO, the ECI gives at least some public control over first steps of decision-making. Though both initiatives are nonbinding, the ECI can – potentially – put more pressure on the EC through Europe-wide campaigns and debates in the European public sphere. Still, the ECI can only influence the first steps of the policy cycle. If and how an ECI will therefore have a real impact on decision-making depends on adaptions taken by the European institutions.

The OC do not offer a forum where different opinions could be exchanged and discussed. It resembles more of a black box into which contributions can be made and picked from by the EC. Real considered judgment cannot evolve in its current design, especially given the lack of transparency. The ECI would offer the opportunity for pan-European communication and deliberation as it addresses an overarching public sphere, but, however, faces in practice struggles with a missing European media landscape. A stronger promotion of the ECI by the European institutions might be a starting point. Considered judgment therefore depends of the establishment of networks within the European public sphere that go beyond usual actors and channels.

Both initiatives are transferable and basically also efficient though they request a high resource input resulting in the distortion of participation in favor of organized and elite CSO.

The ECI clearly comes a lot closer to an ideal web-based form of deliberation than the OC which is not surprising as it was introduced a decade later. But, it has to be kept in mind that even though ICT play a big role in organizing an ECI and collecting signatures, there is still a big divide in how signatures are collected. The OC tool cannot be regarded as an innovative tool in terms of democracy. It might have been one at the point of its introduction but now is in dire need for reforms. Its quality could be easily enhanced by offering additional tools like web forums or webinars on the policy issue to be consulted on. Increasing transparency is also not a question of technical possibilities today but of the willingness of stakeholders.

All in all – have web-based forms of participation led to the development of a European public sphere? The initiatives are addressing different layers of the public sphere. While the OC remains in the realm of segmented public spheres, the ECI addresses an overarching public sphere. A reformed OC would certainly lead to more common action and communication in segmented public spheres, and thus contribute to the development of a European public sphere. This would require

refocusing on CSO participation from all CSO and not only highly professionalized and elitist ones based in Brussels. So far, "even if the OC formally offer the possibility to give qualitative input and enhance the involvement of interested parties, if inclusiveness is not ensured and if it remains unclear who contributes how to the consultation process and how and why arguments are accepted or dismissed, the story of OC remains only one of very confined success" (Quittkat 2011, p. 672).

There are quite clear intentions of the Commission to contribute through the ECI to the development of a European public sphere. In the Explanatory Memorandum to the Regulation on the ECI, it was clearly stated that public debate on European issues shall be promoted even if an initiative might not fall into the framework of the legal powers of the Commission (Monaghan 2012, p. 292). A crucial problem with the emergence of a European public sphere is that there is no real understanding of European citizens for each other in the context of European decision-making. Therefore, there is "little empirical evidence that European citizens view their relationship with EU institutions, or with each other, in a way that would legitimise demos-formation as a strategy" (ibid., p. 295). The question to which extent there can or should be a feeling for being a "community which claims to collective self-determination" remains heavily contested (ibid.). A European public sphere also requires a clear commitment to put sufficient resources into the development of platforms that can reach citizens.

Sociological research shows that elites in the EU are indeed merging into a stronger interconnected community, leaving most of the citizens behind. So far, deliberative procedures cannot be argued to have a "rapid, ground-shaking, substantive impact" (Haidbreder 2012, p. 25). The intended democratizing effect has so far not matched the high expectations and hopes. Whether the ECI can resemble a common activity for all citizens to shape a European identity remains to be seen. Critics point out that the CSO have failed before to mobilize a wider public. However, the ECI enables citizens to actively discuss about European topics and express their opinions by signing an initiative. If and how this will eventually contribute to the emergence of a European public sphere is depending on cooperation of the EU institutions, CSO, and the European citizens.

In conclusion, we can confirm that "ultimately, the ability of online public spaces to revive a genuine public sphere is linked to the capacity of the former to promote the emergence of new ideas in the political debate, their ability to stimulate the appearance of new political communities, and their capacity to foster genuine and inclusive forms of political debate" (Dalakiouridou et al. 2012, p. 318). While the OC clearly fails, the ECI might possess this ability.

Conclusion

Democratic practices based on ICT will need time to gain acceptance as sources of democratic legitimacy. The OC and ECI show that the future might rather see a combination of conventional democratic practices and ICT. This will allow for a

hybrid cyber-public sphere to emerge and maybe lay the ground for a future hybrid cyber-democracy that will evolve alongside with social and technical advancement. But there are many questions that need to be answered and are linked to the overall way forward for Europe as a community of citizens, prosperity, and freedom. A truth in that being that we cannot rely on mere "theoretic modelling" and have to keep in mind that it "is rather the practice of reconstituting democracy in Europe that remains tied to a practice of re-defining the boundaries of the social" (Góra et al. 2012, p. 177).

This analysis confirms earlier findings that EU institutions are developing a positive attitude toward ICT and its role in increasing democratic legitimacy (see Diecker and Galan 2015). Taking a closer look, this might be not the case for every institution and agency. The European institutions will have to keep in mind that their activities will be watched and evaluated by CSO and citizens in regard to the coherence of online strategies and commitment by supplying the necessary resources to really live up to the high expectations that have been raised. Accordingly, the EU institutions and, especially, the Commission have to carefully deal with new technologies, their big potential, and shortcomings, by further developing coherent strategies based on a strong commitment to participation.

The following illustration shall highlight the findings of this chapter. European (Cyber)-public sphere is herein characterized by information flows and exchange in a triangle of actors. These actors interact with each other through established ways of communication. This can include in person meetings, debates, campaigns, and so forth. While this constitutes an established practice, innovations through new mechanisms and communication flows face difficulties to unfold their full potential. In comparison of the democratic innovation through the OC and the ECI, there is a clear advantage for the later instrument of participatory democracy (Fig. 1).

This analysis affirms the conclusion that if the EU fails to properly address and stand up for the development of direct democratic online tools this might lead to

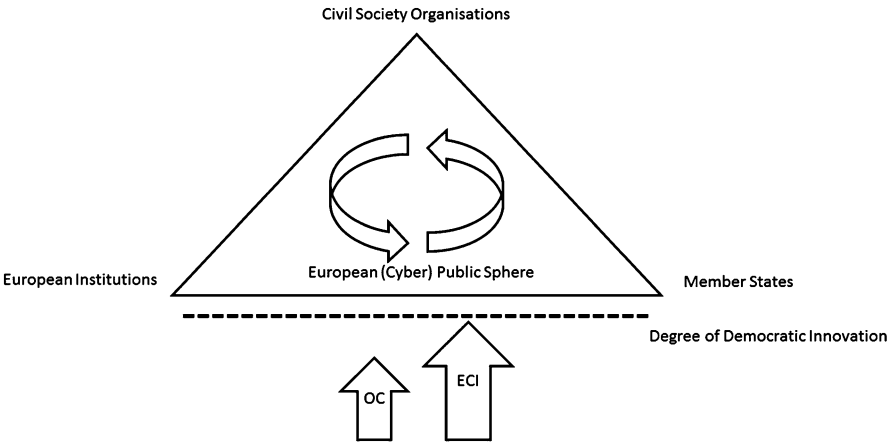


Fig. 1 Source: Matthias Galan

serious disappointment and even bigger loss of legitimacy, driving citizens away from ICT-based solutions. Trust as one of the key elements of democratic legitimacy remains a necessary prerequisite to build reliable tools, which are at the same time user-friendly and up to the security and privacy needs of modern day citizens (see Diecker and Galan 2015).

References

Barker, R. (2007). *Democratic legitimation: What is it, who wants it, and why? In: Hurrelmann, Achim; Schneider Steffen; Steffek Jens: Legitimacy in an age of global politics* (pp. S.19–S.34). New York: Palgrave MacMillan.

Carrara, S. (2012). Towards e-ECIs? European participation by online pan-European mobilization. *Perspectives on European Politics and Society, 13*(3), 352–369.

Cuesta-López, V. (2012). A comparative approach to the regulation on the European citizens' initiative. *Perspectives on European Politics and Society, 13*(3), 257–269.

Dahlgren, P. (2005). The internet, public spheres, and political communication: Dispersion and deliberation. *Political Communication, 22*(2), 147–162.

Dalakiouridou Efpraxia, Smith Simon. (2009). Contextualising public (e) participation in the governance of the EU. *European Journal of ePractice*, *7*. http://www.epractice.eu/files/ePractice-Journal-Volume-7.pdf. Accessed 22 July 2013.

Dalakiouridou, E., Smith, S., Tambouris, E., & Tarabanis, K. (2012). Electronic participation policies and initiatives in the European Union institutions. *Sociel Science Computer Review, 30*(291), 297–323.

De Clerck-Sachsse, J. (2012). Civil society and democracy in the EU: The paradox of the European citizens' initiative. *Perspectives on European Politics and Society, 13*(3), 299–311.

Diecker, J., & Galan, M. (2015). "Creating" a public sphere in cyberspace: The case of the EU. In E. G. Carayannis et al. (Eds.), *Cyber-development, cyber-democracy and cyber-defense: Challenges, opportunities and implications for theory, policy and practice*. New York: Springer Science+Business Media.

Eriksen, O. E. (2009). *The unfinished democratization of Europe*. Oxford: Oxford University Press.

Eriksen, E. O., & Fossum, J. E. (2012). Europe's challenge. Reconstituting Europe or reconfiguring democracy? In O. E. Eriksen & J. E. Fossum (Eds.), *Rethinking democracy and the European union* (pp. 14–38). London: Routledge.

European Commission. (2001). European governance. A white paper. http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0428en01.pdf. Accessed 22 Jul 2013.

European Commission. (2011). Regulation (EU) 211/2011 of the European Parliament and of the Council of 16 February 2011 on the citizens' initiative. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:065:0001:0022:EN:PDF. Accessed 20 Jun 2013.

European Commission. (2015). Report on the application of Regulation (EU) No 211/2011 on the citizens' initiative. COM (2015) 145 http://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-145-EN-F1-1.PDF. Accessed 18 Dec 2015.

European Court of Justice. (2015). Judgment in Case T-450/12 Alexios Anagnostakis v Commission, General Court of the European Union Press Release No. 108/15 http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150108en.pdf. Accessed 10 Jan 2016.

European Parliament. (2015). *Report on the European citizens' initiative (2014/2257(INI))*. Committee on Constitutional Affairs, Rapporteur: György Schöpflin.

Finn, H. V. (2008). Assessing civil society in Europe: Comparative findings of the CIVICUS civil society index. In M. Freise (Ed.), *European civil society on the road to success?* (pp. 45–63). Baden-Baden: Nomos.

Fraser, Nancy (2009): 2. Theorie der Öffentlichkeit. In: Brunkhorst, Hauke (Hg.) Habermas-Handbuch. Metzler: Stuttgart [u.a.]. S.148–S.155.

Freise, M. (2008). The civil society discourse in Brussels – between societal grievance and Utopian ideas. In M. Freise (Ed.), *European civil society on the road to success?* (pp. 23–43). Baden-Baden: Nomos.

Friedrich, D. (2008). Actual and potential contributions of civil society organisations to democratic EU-governance. In M. Freise (Ed.), *European civil society on the road to success?* (pp. 67–86). Baden-Baden: Nomos.

Garcia, L. B., & Del Río Villar, S. (2012). The ECI as a democratic innovation: Analysing its ability to promote inclusion. Empowerment and responsiveness in European civil society. *Perspectives on European Politics and Society, 13*(3), 312–324.

Góra, M., Mach, Z., & Trens, H.-J. (2012). Situating the demos of a European democracy. In O. E. Eriksen & E. J. Fossum (Eds.), *Rethinking democracy and the European Union* (pp. 159–178). London: Routledge.

Greenwood, J. (2012). The European citizens' initiative and EU civil society organisations. *Perspectives on European Politics and Society, 13*(3), 325–336.

Habermas, J. (1997). *Die Einbeziehung des Anderen: Studien zur politischen Theorie*. Frankfurt am Main: Suhrkamp.

Habermas, Jürgen. (1998) [1992]. Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats. Frankfurt/Main: Suhrkamp.

Haidbreder, E. G. (2012). Civil society participation in EU governance. *Living Reviews in European Governance*, *7(2)*, http://europeangovernance.livingreviews.org/Articles/lreg-2012-2/download/lreg-2012-2Color.pdf. Accessed 22 July 2013.

Hurrelmann, A., Steffen, S., & Jens, S. (2007). *Legitimacy in an age of global politics*. Basingstoke: Palgrave MacMillan.

Karr, K. (2006). *Democracy and lobbying in the European Union*. Frankfurt: Campus Verlag.

Kies, R. (2010). *Promises and limits of web-deliberation*. Basingstoke: Palgrave MacMillan.

Möllers, Christoph (2009): 13. Demokratie und Recht. In: Brunkhorst, Hauke (Hg.): Habermas-Handbuch. Metzler: Stuttgart [u.a.]. S.254–S.263

Monaghan, E. (2012). Assessing participation and democracy in the EU: The case of the European citizens' initiative. *Perspectives on European Politics and Society, 13*(3), 285–298.

Quittkat, C. (2011). The European Commission's online consultations: A success story? *Journal of Common Market Studies, 49*(3), 653–674.

Rasmussen, Anne, & Toshkov, Dimiter. (2013). The effect of stakeholder involvement on legislative duration: Consultation of external actors and legislative duration in the European Union. *European Union Politics 14*, 366–387.

Rogg, A. (2003). *Demokratie und Internet: der Einfluss von computervermittelter Kommunikation auf Macht, Repräsentation, Legitimation und Öffentlichkeit*. Opladen: Verlag Leske + Butrich.

Schmalz-Bruns, Rainer (2009): 15. Demokratie. In: Brunkhorst, Hauke (Hg.): Habermas-Handbuch (pp. 75–81). Metzler: Stuttgart [u.a.].

Seybert, H. (2012). *Internet use in households and by individuals in 2012*. Eurostat Statistics in Focus 50/2012. http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-12-050/EN/KS-SF-12-050-EN.PDF. Accessed 24 July 2012.

Seybert, H., & Reinecke, P. (2014). *Internet and cloud services – statistics on the use by individuals*. Eurostat Statistics in focus 16/2014. http://ec.europa.eu/eurostat/statistics-explained/extensions/EurostatPDFGenerator/getfile.php?file=77.163.203.106_1450459938_26.pdf. Accessed 18 Dec 2015.

Smith, G. (2009). *Democratic innovations: Designing institutions for citizen participation*. Cambridge: Cambridge University Press.

Szeligowska, D., & Mincheva, E. (2012). The European citizens' initiative – empowering European citizens within the institutional triangle: A political and legal analysis. *Perspectives on European Politics and Society, 13*(3), 270–284.

Consumerization of IT, Cyber-Democracy, and Cyber-Crime: The Inherent Challenges and Opportunities of Two Ends of a Continuum

28

Birgit Eigelsreiter

Contents

B. Eigelsreiter (✉)
Ministry of Health and Women's Affairs, Vienna, Austria
e-mail: birgit.eigelsreiter@outlook.com; birgit.eigelsreiter@frauenministerium.gv.at; bmitterlehner@psr-institut.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_9

Abstract

Consumerization of IT has introduced multidimensional social changes which require a mature security response that is risk-based and demands a high degree of sophistication. As technologies became democratized and societies got equipped with a plethora of high-potential technologies with which to access the Cyber-Space at any time, communication and action patterns would thoroughly change and alter our spheres of professional and private life, agenda setting, political participation, and behavioral patterns. While security issues are being put on the back burner, cyber-rebels and cyber-criminals grow in numbers. New risks and challenges ensue from this.

Therefore, this chapter assesses potential advantages and risks of the Cyber-Space in terms of Cyber-Democracy and Cyber-Crime, inclusive of the latest trend of Bring-Your-Own-Device (BYOD). It illustrates that cyber-democratic action and participation are wide concepts that extend beyond classical definitions of democratic participation and emphasizes the importance of bottom-up mobilization and agenda-setting. At the same time, it underlines how freedom of expression and Cyber-Crime interact by using the example of hacktivism and the hacker movement Anonymous.

Even if technological (device management) methods and strategies may help cope with these challenges, they are not an entirely technical issue. This is illustrated by the trend of Bring-Your-Own-Device, where issues at stake also concern legal questions as well as psychological ones (awareness, negligence, and willingness to face existing challenges). Therefore, this chapter also pays attention to the manifold legal issues which have been unsolved so far and urges for legal measures to fill the existing gaps and loopholes pointed to.

Keywords

Cyber-Democracy · Cyber-Crime · Cyber-Governance · Bring Your Own Device (BYOD) · Cloud computing · Consumerization of IT · CoIT · Anonymous · Wikileaks · Pirate Party Movement · Private Cloud · Public Cloud · Knowledge worker · Workplace democracy · Data protection

Introduction

When Friedman assumed that globalization would go hand with hand with democratization of technology and information as of 1999 (Friedman 1999) he was to be right: In fact, the last decades have coined a new communication and innovation paradigm with the impact of technologization and digitalization on our society being as important as the invention of the book (Fig. 1) (Moore 2011; Niehaves et al. 2012; Harris et al. 2011).

This paradigm shift was found to have its origins in what is popularly referred to as Consumerization of IT (CoIT): (Baskerville 2011, p. 251ff; Moschella et al. 2004, p. 12; Choucri 2000, p 248–252). (Examples of CoIT comprise both software and hardware and include: Smartphones, tablet PCs, cloud services (Google (e.g., Drive,

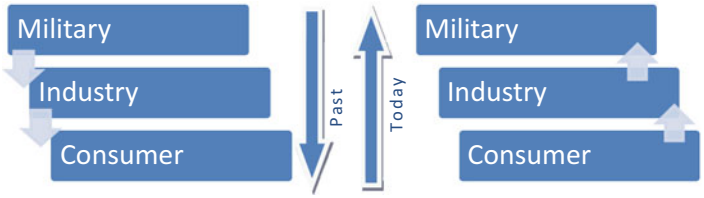


Fig. 1 Paradigm change in ICT use (based on Mitterlehner 2014, p. 212)

Calendar, Mail, Apps)/Microsoft SkyDrive/OwnCloud/Dropbox/CloudME), facebook, etc. (See Mitterlehner 2014).) Among other factors, strong liberalization policies in the area of telecommunications. For instance, the telecommunications sector was the first one to be liberalized (starting with the liberalization of end user devices) in the European Union (Klöpfer and Neun 2000); Liberalisation of the media (which led to mass production of ICT and affordable prices for end users and civil society) as well as mass production have provided powerful and user-friendly information and communication technologies (ICT) to society at large in an affordable way and, thus, transformed the Cyber-Space into a universally accessible space.

This being so, ICT and the Cyber-Space – with the Internet as the most influential breakthrough – have added a cyber-dimension to our lives and thoroughly changed upheld values, approaches, and ways of thinking, work, and interaction (Harris et al. 2011: 2ff; Klöpfer and Neun 2000; Mitterlehner 2014; Poster 1995). While Web 1.0 technologies have altered traditional communication means and paths as well as the scope for knowledge societies, Web 2.0 technologies go one step further. They may strengthen inclusive democracies as they give a voice to people independent from their place and the condition they are in, or from their cultural, linguistic, or ethnical backgrounds, and allow them to access, interpret, share, treat, and process knowledge and information in new ways (e.g., social networks, chats, blogs, etc.) (Clarke et al. 2012b; Castells and Cardoso 2005: 13ff; Heckmann 2011). Consequently, a new paradigm has entered our society changing all kinds of communication and action patterns (Papacharassi 2010); new and innovative communication possibilities have profoundly changed traditional communication and action patterns (i.e. postal mail, shopping, payment transactions). As technologies became democratized and societies (particularly the industrialized nations) got equipped with a wide range of high-potential technologies with which to access the Cyber-Space at any time (Sambharya et al. 2005) – with the Internet as one of the most important infrastructures (see for instance Odlyzko 2003; Moore 2011; Niehaves et al. 2012; Harris et al. 2011) that has become a backbone of the industry as well as civil society. This broadens the options in terms of knowledge democracies. In particular, the invention of Web 2.0 has leveled the playing field of public dialogue by allocating communicative tools in a more egalitarian manner and complementing conventional democratic and societal structures. New bottom-up or horizontal communication modes have ensued, which have a lasting impact on social, economic, and political settings. By way of example, Xavier and Campbell argue that Social Media were primordially responsible for the Arab spring (Xavier and Campbell 2014, p. 153).

In fact, the Cyber-Space, telecommunications, and Internet services have become an integral part of services of general interest – the EU-term describing essential services in a society (Mitterlehner and Barth 2013; Mitterlehner 2013) which – according to the Charter of Fundamental Rights of the European Union – must be provided in a universal, comprehensive and affordable way as well as at high quality (CFR: Art. 36; TFEU: Protocol 26). These stipulations are abided by the European Union in that it fosters universal access to the Internet as well as a harmonized set of data policies in its policies (e.g., by means of the Digital Agenda) (Digital Agenda 2010). And not only is this so, but as other communication networks (such as classical telephone networks) decline in importance the Internet is turning into an ever more important medium (Collins 2001; Markopoulou et al. 2002, 2003). Naturally, this paradigm shift also comes with drawbacks. A certain dependency on the availability of the Internet and ICT (also for running critical infrastructures) entails from their omnipresence and new risks and challenges emerge. Still, as providers and producers face high competition and market pressures and give in to the demands of CoIT and commercialization, they have put security aspects on the back burner; even more so as the latter are not being perceived as an added value by most users in contrast to other features such as functionality and intuition. What is more, (further) developing security standards needs thorough work and research; more often than not, it might seem easier (also in terms of marketing) to put a new generation of devices on the market (on this, see also Cavelty 2012).

1. In which ways has Consumerization of IT influenced the potential of Cyber-Democracy and Cyber-Crime?
2. How far does Cyber-Democracy go?
3. BYOD – Vice or Virtue?

In order to answer these research questions, this chapter is divided into the following subchapters: First, a small encyclopedia (based on [Mitterlehner 2014]) and a synopsis of cyber-concepts and vital terms is meant to introduce the subject. Second, the scope of ICT for Cyber-Democracy is presented and compared to its inherent security challenges. Finally, one chapter is dedicated to one particular trend: BYOD. A particular emphasis is to put on legal aspects challenges connected to a global virtual space.

Terminology

Bring-Your-Own-Device (BYOD)

A trend which has its origins in CoIT. It refers to the use of private end-devices for professional activities. In this chapter, BYOD refers to employees using their private end-devices and privately used public consumer applications and software, such as public clouds (e.g., Dropbox, Apps), for professional reasons (with or without the employer knowing and approving thereof) (Gilbert 2012, p. 39; Oppliger 2011; Lennon 2012).

Cloud Computing

"*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*" (NIST 2011, p. 2f). It is characterized by five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), three service models (SaaS, PaaS, IaaS), and four deployment models (private, community, public, and hybrid cloud) (NIST 2011). Using storage capacities of a server network, it is a flexible instrument that hides economic advantages. Today, business data storage is popularly being outsourced to clouds (public or private ones). However, cloud attacks are particularly hazardous as clouds represent a "single point of failure."

Cyber-Democracy

A desktop research reveals that cyber-democracy, e-democracy, cyber-politics, and e-politics are frequently used synonymously. Often, those terms are used for theories of how new ICT may drive and further democratic processes. Given the openness of the Cyber-Space and the power it grants to the general public, it can be a sound tool to further democratic citizenship. This chapter assumes that the concept of Cyber-Democracy goes beyond e-voting. In particular, the expressions of discontent or political aggression as a means for democratic citizenship in the Cyber-Space are assessed in this chapter.

Cyber-Space

The totality of all communication networks, databanks, and information sources stored and exchanged electronically. The Internet is part of the cyberspace, yet, not synonymous to it (Cavelty 2012, p. 3f). However, this chapter particularly refers to the Internet when using the term Cyber-Space.

Cyber-Security

"*Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.*" (ITU-T 2008, p. 2f)

This term denotes both, a status and a process targeted at the mitigation and resolution of all risks related to the Cyber-Space. It includes political, technical, administrative, legal, and any other countermeasures to a threat. A secure Cyber-Space grants integrity, confidentiality, and authenticity of information (ITU-T 2008).

Consumerization of IT (CoIT)

There are distinct definitions of CoIT. Murdoch et al. describe the phenomenon of "*abandoning enterprise IT – both hardware and software in favor of consumer technologies that promise greater freedom and more fun*" (Murdoch et al. 2010, p. 2). Harris et al. refer to this paradigm as "*the adoption of consumer applications, tools and devices in the workplace*" (Harris et al. 2011, p. 3). BYOD is a side-effect thereof; employees have started to revert to using their consumer applications instead of (probably more secure) business ICT-frameworks (e.g., by using iPhones, Dropbox, etc.) (Harris et al. 2011, p. 4ff). This chapter relates to CoIT as a process where IT is conceived in a customer-friendly and marketable way.

Knowledge Worker

In this chapter, knowledge worker means any staff whose main capital is knowledge. In terms of cyber-security, it means that they have access to, use, or produce explicit or documented knowledge and classified information of an organization.

Open Government

"The transparency of government actions, the accessibility of government services and information, and the responsiveness of government to new ideas, demands and needs" (Karamagioli 2013), improving the evidence base for policy making, strengthening integrity, discouraging corruption, and building public trust in government. As such, governance systems become more responsive as information flows freely both to and from governments through different channels.

Organization

Any business, company, or organization – be it under private or public law.

Private Cloud

May be run internally or by a (third party) provider. The advantages of a cloud cannot be fully exploited in a private cloud and the degree of Consumerization may be limited. Yet, data security is higher in comparison to public clouds, as in public clouds a successful attack of a cloud will affect all data (NIST 2011).

Public Cloud

Services are provided by an external provider and are available to the general public. Scalability and resource pooling can be fully exploited in a public cloud, yet, risks of

data loss due to an attack or data transmittance to the provider and subcontractors are higher. As in all clouds, an attack will affect all data (NIST 2011).

Risk

A "Threat which abuses vulnerabilities of assets to generate harm for the organization" (ISO/IEC 27005).

Agenda-Setting, Information and Knowledge Production, Processing, and Sharing at the Heart of Cyber-Democracy

Even though in the beginning of the cyber-age, the *academia* would forecast a broadening information gap (also referred to as digital divide) between social groups well-versed in ICT and those who are note (Benton Foundation 1998; DiMaggio and Hargittai 2001) and even though there first was and still partly is a digital divide between those who have access to ICT and those who have not (Hammond 2001; Choucri 2000; Chen and Wellman 2005) such doubts have proven unfounded. In particular, this applies to industrialized countries where existing digital divides have been shrinking (see Eurostat 2013 for data in Europe) and are supposed to continue to do so even further in the future (Chen and Wellman 2005). (The use of the Internet by the economy, administration, and society is above the European average in Austria. This is due to a strong roll-out of Internet infrastructure (e.g. broadband) and an expansion of its use (e.g., e-commerce, e-government, etc.) (Kompetenzzentrum Internetgesellschaft 2013)).

An increasing ICT competence and ICT literacy (also due to the integration of ICT in our mundane activities as described above) has an impact on awareness-raising (e.g., transnational policies), agenda-setting, and social relations of power (e.g., Arab spring) by adding new opportunities to systems and methods or processes of information distribution and knowledge creation, dissemination, and processing (Leiner et al. 1997) (For more information on how Cyber-Democracy has influenced the Arab Spring, see also Xavier and Campbell (2014).). The scope and potential for manipulation and agenda-setting through search engines (e.g. hits based on popularity, hits paid for in the background) shall be pointed out in this regard particularly their influence on mind-setting, society and [prevailing] opinions, yet this will not be discussed in this chapter. It should also be outlined that hits based on popularity are likely to promote mainstream thinking so that search engines programmed this way automatically marginalize nonmainstream approaches.

Even though the Internet might not be as free as it seems at first glance, it offers a new medium for transporting contents which may be used indifferent of occupation, social stratum, ethnic background, age, etc. Being empowered by ICT and the Cyber-Space, users are no longer passive consumers, instead, they can challenge "the monopoly control of media production and dissemination by state and commercial institutions" and make their voices heard (by pointing to or developing alternative opinions and solutions globally) via official and informal channels, which provide a

platform for the exchange of opinions and ideas in synchronical ways regardless of space and time (Klein et al. 1999; Loader and Mercea 2011; Klein et al. 1999; Papacharassi 2010). As such, Cyber-Democracy may be viewed as one form of knowledge democracy. (Campbell et al. 2015).

Some go as far as to say that open governments bring about citizen-friendly governments where policies are shaped by and in the interest of citizens. This fits in with the approach to compare the single spheres of action (academia, industry, civil society, media [and the Cyber-Space]) to helices interacting with each other fluidly and dynamically (Campbell and Carayannis 2014, p. 126; on the helix models acccording to (Gibbons et al. 1994; Etzkowitz and Leydesdorff 2000)) and further developed by Campbell and Carayannis, see also Carayannis and Campbell (2009), (2010), Barth (2011), Carayannis et al. (2012). Furthermore, it could be used to foster identification with the European project – one of the EU's prime challenges. This has even been addressed at primary law level in the Treaty on European Union (TEU):

"Every citizen shall have the right to participate in the democratic life of the Union. Decisions shall be taken as openly an closely as possible to the citizens"(art 10 para 3 TEU), whereby institutions shall "by appropriate means, give citizens and representative associations the opportunity to make known and publicly exchange their views in all areas of Union action" (art 10 para 3 TEU in combination with art 11 para 1 TEU).

Unsurprisingly, the last years have been marked by attempts to increase and foster political participation and political dialogue via Cyber-Democracy tools (Klein et al. 1999), whereby there are different levels at which to intervene (e.g., online surveys, online mobilization, e-government, etc.). Taking for instance, the traditional distinction between participatory (sometimes called direct or deliberative), representative (or indirect) and plebiscitary democracy, it is important to note that Cyber-Democracy can manifest itself in any of the different types of democracy (and even beyond them. Nevertheless, rather than describing the Internet as inherently democratic it should be viewed as a facilitating tool "which can be turned to repressive and non-democratic ends" (Barber 1999). In terms of democracy, it may enhance participatory democracy as it increases government accountability and transparency through (Williams 2006):

- The provision of government services (e-government services such as voter registration, car registration, etc.) and information
- The provision of information during election campaigns (web presences allow candidates to express their perspectives on the issues, solicit funds, and seek volunteers/mobilize support) as well as to criticize and satirize their opponents
- The opportunity to seek other sources and perspectives through the Internet
- Civil participation by means of computer-mediated communication to voice opinions (possibility to protest issues across political boundaries, and even to mobilize transnationally)
- Internet-based voting, etc.

As a result, it is no longer sufficient to distinguish between democracies and non-democracies (Campbell and Barth 2009, p. 210; Campbell et al. 2015). Instead,

a more substantiated approach of democracy and democratic participation (which surpasses voting, party membership, petitioning representatives) featuring the distinct qualities of different democracies is required (Campbell and Carayannis 2014, p. 128).

Assessments ought to take account of the influence of social diversity, discontent, inequalities, and cultural differences as well as their potential for democratic innovation (Loader and Mercea 2011). This view is supported by Squires who argues for an approach that "recognizes the multiplicity of identity positions that citizens are required to grapple with in contemporary societies, where the spheres for democratic engagement reach into the private spaces to enable the personal to become political" (Squires 1998). Also, Campbell and Barth point out that there are multiple wider and narrower ways of defining democracy and democratic action in their comparative analysis of measurements featuring democracy and democratic quality (Campbell and Barth 2009) (The majority of democracy measurements include, besides other factors, education.). Besides looking at distinct possibilities of expanding existing institutions such as the ones of a representative democracy or the discursive power of existing political theories, it is also worthwhile to take into account other organizing and mobilizing powers and efforts (Poster 2001, p. 173).

Nonetheless, the acquisition of a tablet, a smartphone, or a laptop does not necessarily entail political participation, even if, in theory, it adds to the set of possibilities of democratic participation, active citizenship (by means of forums, blogs, e-voting, etc.), and passive citizenship (by seeking information about political programs, etc.). Neither does permanent access to social media. Different authors point to the fact that it is mostly those who are already fully committed to political causes (activists, party members, etc.) who are cyber-democrats. This would lead to the assumption that new phenomena such as the Arabian spring are a new form of mobilization of politically active and motivated people rather than the result of a new democratization through cyber-possibilities (Rettberg 2008). Therefore, it has provoked controversy if Cyber-Democracy is really that much a panacea and apt to meet today's problems such as disenchantment with politics and if it will really help rach groups beyond those who are committed democratic participants (Castells and Cardoso 2005). Besides questions revolving around a potential digital divide, questions on different returns on Cyber-Democracy have to be put forward in order to understand "the mechanisms, consequences, and institutional context of inequality in access to the Internet and use of the services it offers" (DiMaggio et al. 2004, p. 563).

Any controversial opinions on this issue notwithstanding, it is very much likely that the Cyber-Space may have at least a certain positive impact, notably among younger generations even if the "democratizing effect" of the Cyber-Space cannot be fully proven (see Loader and Mercea 2011; Baron 2008; Brandtzaeg and Heim 2009; Livingstone et al. 2011; Dahlgren 2009).

The Pirate Party (movement) is one of the most shining examples of how the Cyber-Space and a digital generation may upset traditional forms of political parties and democracy (see also Mitterlehner 2014 on this). This is illustrated not only by its party program but also by the variety of digital participation forms (e.g., internal and external discussion platforms, wikis, forums, feedback loops, etc.) implemented within the party.

Another, more controversial, example that goes beyond (cyber-) political party activities is the Anonymous movement (Chiarella 2013, p. 28). It denotes a movement of hackers who would describe themselves as a leaderless idea rather than a group (Chiarella 2013, p. 28) or as an "anarchic global brain connected by various spaces on the Internet" (Hai-Jew 2013, p. 52). The movement does not act as a group. As infiltration (by authorities) is high, no one can trust another within the group. Being a lightly structured network, Anonymous benefits from low investment costs for entry, virtual anonymity, ease of exit, and asymmetrical vulnerability, yet, it is prone to legal and illegal coercion by governments and organizations if caught (Hai-Jew 2013, p. 57). It would go too far to assess the existence of ideological superstructures scaffolding a worldview or any social or political ideology or program at Anonymous (which it actually denies to uphold), yet liberating access and ownership of or to information clearly is one of their key goals and values.

Anonymous is one example of how blurred the line is when it comes to distinguishing between democracy in action and domestic cyber-terrorism: While their actions are illegal in nature and law, they do not launch any violent activities as would be typical for terrorist actions. There are also some democratic elements, as freedom of speech on the computer is permitted by and within Anonymous (Chiarella 2013, p. 31). This will be discussed more closely in one of the subchapters.

Democratic Action or Security Risk? Where to Draw the Line Between Freedom of Opinion, Knowledge Processing, Disruptive Actions, and Expressions of Discontent

Cyber-Democracies respond to the perpetual need for reinvention of democracies, for "earlier ideas about an electoral democracy are becoming outdated and will not suffice in today's era" (Campbell and Carayannis 2014, p. 123). As highlighted above, democratic action is more than just voting and it is independent from party membership. Thus, the Cyber-Space should rather be viewed as "an empty space or institutional void in which tensions between state-centric and democratic citizenship can be played out" (Coleman and Blumler 2009, p. 7). Therefore, Mitterlehner proposes that each single piece of content in the Cyber-Space is information and may be transformed into tangible knowledge and, as such, be used by empowered citizens. In this regard, multifaceted information distribution channels – be it YouTube content, social media, blogs, newspapers, academic research, etc. – must be given the same degree of attention and weight as other channels when attempting to revive democratic action or to analyze democracies, political agendas, and (dis)content (Mitterlehner 2014). Supporting this view, Coleman and Blumler point to the variable of "critical citizenship and radical energy" as a form of democratic citizenship (Coleman and Blumler 2009, p. 3).

As a consequence, it may be assumed that virtually any form of expression in any of the different spheres of action, even explicitly nonpolitical ones,

disruptive activities, and expressions of discontent (YouTube videos, protest music, blogs), are expressions of democratic citizenship (Loader and Mercea 2011). However, it is difficult to draw the line between Cyber-Democracy and Cyber-Crime when assessing the democratic power of expressions of discontent and disruptive activities: Which kind of expression of discontent and sharing of information may be considered democratic and which one may be considered to be a crime?

Hacktivism is one serious problem in this regard as it has introduced "a brave new world of activism" and "(electronic) civil disobedience" (Goodrum and Manion 2007, p. 62). Its measures and actions are to be classified somewhere between cyber-democratic action and Cyber-Crime, whereby the act of (electronic) civil disobedience "entails the peaceful breaking of unjust laws" (Goodrum and Manion 2007, p. 62). Qualifying hacking as an act of civil disobedience if hackers are clearly motivated by ethical concerns, nonviolent, and ready to accept the repercussions of their actions (whereby it is unclear if these characteristics need to be met in a cumulative way) (Goodrum and Manion 2007, p. 64), Goodrum and Manion allocate the following properties to hacktivism (Goodrum and Manion 2000, p. 15):

- No damage to persons or property
- Nonviolence
- No personal profit
- Existence of an ethical motivation, e.g., the strong conviction that a law is unjust, unfair, or to the detriment of the common good
- Willingness to accept personal responsibility for outcome of actions

Therefore, it is necessary to distinguish between Cyber-Terrorists as being those who use computer technologies with the intention to cause grave harm and hacktivists (Goodrum and Manion 2007, p. 63) who pursue some kind of meta-goal with their "harmful" actions that can be summarized as follows (summarized by Levy 1984 in Himma 2007, p. 94):

- Unlimited and total access to computers
- All information is free
- Decentralization and mistrust of authorities
- Computers can change lives for the better
- Hackers should be judged by their hacking, not by any bugs, age, race, or position
- You create art and beauty on a computer

Regardless from their motivation and the scope of their actions, members of Anonymous (and those helping them) as well as any other hackers come into conflict with the law every time they hack into a computer; one exception is ethical hacking, where the goal is to stop regular hacking (Chiarella 2013, p. 28f). In this regard, Nye distinguishes between three faces of power in the Cyber-Space (Nye 2010, p. 7):

- A makes B do what B would initially or otherwise not do (means of hard power: denial of service attacks, insertion of malware, CADA disruptions, arrests of bloggers; means of soft power: information campaigns to change initial preferences of hackers, recruitment of members of terrorist organizations)
- A precludes B's choice by exclusion of B's strategies (agenda control; means of hard power: firewalls, filters, and pressure on companies to exclude some ideas; means of soft power: ISPs and search engines of self-monitor, ICANN rules on domain names, widely accepted software standards)
- A shapes B's preferences so that some strategies are never even considered; (means of hard power: threats to punish bloggers who disseminate censored material; means of soft power: information to create preferences (e.g., stimulate nationalism and "patriotic hackers"), develop norms of revulsion (e.g., child pornography))

Anonymous mostly stresses soft power (the effect of persuasion through messaging) rather than hard one (by using information instruments within the Cyber-Space), for instance, by launching Denial of Service (DOS) attacks or by using information in a soft way in order to create preferences among hackers and to affect norms of revulsion. As a result, their attacks cause information loss and public humiliation which might entail instability, system disruption, reputation loss, and intellectual property theft (Hai-Jew 2013, p. 57ff).

The polarity of this issue is also reflected by Wikileaks' disclosure of government secrets which started out as a disclosure of classified information of other countries already known to state authorities due to their own information policies (Leigh and Harding 2011), or by distinct acts of national espionage which have popped up. As a result, the sovereign (usually the state) is struggling with granting everybody their fundamental rights of expression and participation while ensuring national security: How to protect states, businesses, and citizens without infringing their freedom of expression and action?

Another problem with hacktivism that goes beyond difficulties in categorizing disruptive actions (and one another reason why it is that difficult to draw the line between the different categories) is that world havoc could ensue from it when spin-off groups conducted attacks or grew in power (e.g. through crowd-funding). Consequently, any "good" intentions notwithstanding, all these activities (and naturally also any form of Cyber-Crime) could have major impacts on vital sectors of the economy, inclusive of shut-downs of power grids and critical infrastructures as we have become an ICT-dependent society (Hai-Jew 2013, p. 55; Eriksson and Giacomello 2006). This includes telecommunications, power, transportation, banking, water supply and sewage, etc.

Privacy Data Protection Acts or Electronic Privacy Acts serve the purpose of protecting data and online movements. In addition, one can help oneself with added physical security, procedural security, environmental security, encryption, better password security, multivariable authentication or SSL protection. Furthermore, law enforcement does have traceback and forensic capabilities. It is possible to identify where individuals entered the Internet, which paths or which bouncepoints they took

to arrive at target computers, as well as to trace hacker actions in virtual audits which trail into the ether. Yet, the challenge is to get law enforcement involved. This requires clear indicators of when hackers have crossed the line into criminality in their vigilant actions (unlawful access to private intellectual property, illegal interception of information, impersonation of another, unlawful use of telecommunication equipment, forgery, theft of property, breaking into private systems and networks, violation of privacy, threats, Distributed Denial Of Service(DDOS) attacks or SQL injection attacks). As a response to hacking, anti-cyber-crime bodies have been established that meet evidentiary standards in the collection of digital information while protecting citizens' privacy and other First Amendment rights.

Implications for Practice: Bring-Your-Own-Device – Vice or Virtue?

It was CoIT which made ICT devices affordable, interoperative, and compatible and which laid the foundation for trends such as flexicurity, home office and mobile office, teleworking, and e-learning (Martinez and Rajlkshmi 2012). Only so could concepts of knowledge economy and work-life balance translate into work-flexibility (Maier et al. 2008; Price Waterhouse Coopers 2011, p. 4). Everything this entails – the Cyber-Space, electronical data processing, digitization, technologization, and real-time communication – has not only completely changed our way of thinking but also our approaches to work (life) and leisure (Klöpfer and Neun 2000). In particular, this paradigm shift has sharpened the profile of the knowledge worker who works on a performance- or project-based level from any place by using the office the home office and the mobile office (which is everywhere), as possible work places (Martinez and Rajlkshmi 2012) at any time in theory (Entity Solutions 2013). Based on personal responsibility and independence at work, the concept of work-flexibility may become an integral part of the concept of a democratic workplace: The knowledge worker is free to assign internalized resources, energy, capacity, capability, and competence to the different tasks needed to accomplish their goals. Accordingly, they are granted autonomous authority to make decisions and take independent actions within their fields of work (Olsen 2009).

Other than classical participatory instruments, work-flexibility means that the knowledge worker is free to assign internalized resources, energy, capacity, capability, and competence to the different tasks needed to accomplish their goals. Accordingly, they are granted autonomous authority to make decisions and take independent actions within their fields of work (Olsen 2009). Consequently, based on personal responsibility and independence at work, the concept of work-flexibility is an integral part of the concept of the democratic workplace.

One trend that has emerged alongside with all this is Bring-Your-Own-Device (BYOD): While BYOD is often being used synonymous for CoIT, this chapter distinguishes CoIT from BYOD in a way that it exclusively refers to employees/knowledge workers using "their" consumer devices and applications for professional purposes (Maier et al. 2008; Price Waterhouse Coopers 2011, p. 4). In India, the

Table 1 Working attitudes (based on Mitterlehner 2014, p. 218)

	Private purpose	Business purpose
Private ownership	Use of private IT for private purposes	BYOD (e.g., use of private smartphones to access business email accounts)
Business ownership	Use of business IT for private purposes	Traditional use of business IT for work

Netherlands, and the USA virtually 30% of the active population already use their own devices for professional activities; in Europe, there is more reluctance to do so (Stork et al. 2012). Other sources use even higher estimates for this trend (CIO 2013). Even if we do not have exact figures, it is likely that this trend will increase in Europe (Clarke et al. 2012a; Price Waterhouse Coopers 2011, p. 3). As there are numerous definitions, it is not clear if BYOD exclusively refers to company policies or also to negligent (non-)uses of commercial (private) end-devices and applications which are compatible with professional ones and *vice versa* (see also Mitterlehner 2014). Table 1 illustrates the differences to "traditional" ICT models at the workplace.

While its definition has provoked controversy, its benefits have not: BYOD is alleged to increase efficiency, creativity, and motivation (see also Andriole 2012: "[...] there's a reverse technology - adoption life cycle at work: employees bring experience with consumer technologies to the workplace and pressure their companies to adopt new technologies.") so that workers may be reached even in their leisure time (calls, e-mails, downloading information/materials) (Drury and Absalom 2012; Clarke et al. 2012b, p. 15ff): BYOD thus helps save resources and democratize the workforce. As such, BYOD may seem to be an attractive solution for both, employers and employees: It offers the advantages of reduced resource spending (yet, there are hidden costs for the organization which should not be overlooked if the use of private end-devices is accompanied by a BYOD policy (Rose 2013; Kaneshige 2012)), operational optimization (e.g. by means of remote-working), higher productivity (e.g. due to higher mobility and permanent access to professional data), higher employee competence, and higher creativity (Drury and Absalom 2012; Clarke et al. 2012b, p. 15ff). Furthermore, BYOD allows employees to reconcile their professional and private lives. In India, the Netherlands, and the USA, virtually 30% of the active population already use their own devices for professional activities (other sources use even higher estimates for this trend (CIO 2013)); in Europe, there is more reluctance to do so (Stork et al. 2012). Unclarities about exact figures notwithstanding, it is likely that this trend will increase in Europe, too (Clarke et al. 2012a; Price Waterhouse Coopers 2011, p. 3). Andriole refers to this phenomenon as follows: "[...] there's a reverse technology adoption life cycle at work: employees bring experience with consumer technologies to the workplace and pressure their companies to adopt new technologies" (Andriole 2012).

However, from a security point of view, the use of consumer end-devices and applications for professional purposes presents high security risks (e.g., hacking, loss, theft, phishing, malware, spying, etc.) (Infosecurity Magazine 2012; Clarke et al. 2012a, b; Niehaves et al. 2012, p. 10; Stork et al. 2012). Any abuse or attack may

prove detrimental to the organization concerned; consumerized devices increase those security risks (Clarke et al. 2012a, b). While professional devices take account of security issues and are based on a server from which data is usually centrally managed, consumer devices and applications may neglect security aspects as they are not designed for professional usage but supposed to feature the facilitated use of multimedia content (for private purposes).

So far, most contributions on this issue have dealt with company risks (ENISA 2012a, b). However, one should also include in such an analysis the dimension of the state and state organizations. Data thieves in the modern (e.g., hackers, skriptkids, etc.) or in the traditional sense (e.g., theft of hardware) attempting to get access to classified information might make use of this security gap; business data or classified information may leak through to third or non-authorized parties deliberately or inadvertently for reasons of nonproper use by the worker (e.g., if stored on public clouds like Dropbox or if handed to third parties [e.g., private laptop or smartphone is broken and is sent to a third party to repair it] or lost), publication on facebook, providing access to third parties by not using a safe password or by loss of device, or attacks (e.g., hacking, malware, etc. or physical attacks such as theft) (Clarke et al. 2012a; Niehaves et al. 2012, p. 10). Also, if data storage has been outsourced, information may end up on servers in other countries with less stringent data protection legislation. Under this angle, BYOD may have serious effects. If incidents occur within the scope of the sovereign state (classified information) or with regard to usually state-owned or state-controlled fundamental services – such as water, electricity/energy companies – this may even affect society at large (Mitterlehner and Barth 2013).

In fact, 13 of 22 chapters scrutinized by Niehaves et al. revealed major weaknesses in data security (Niehaves et al. 2012, p. 6). Other papers pointed to security risks in BYOD, too (e.g. Aerospace Industries Association 2011, p. 5ff). Risk mitigation is difficult – especially if the organization lacks awareness in the first place. Also, a "No-COIT/Private Device-Policy" does not foster immunity to any risks. Employees may still (negligently) use private end-devices and applications (e.g. store information on public clouds) if they wish to retrieve this information when not in office (so that the compatibility of different end-devices becomes a vice). Yet, as for now, national security policies have neglected the issue of BYOD. By way of example, Austrian legislation and security strategies deal with clouds and cyber-security, yet have neglected the issue of BYOD and are but one example of how BYOD is underestimated (Digitales Österreich 2012). Consequently, the present state of supervisory control may not be commensurate with the vulnerabilities, threats, and their potential consequences (Aerospace Industries Association 2011; Clarke et al. 2012a).

Table 2 summarizes the advantages and disadvantages of using private consumer devices and applications for professional purposes in accordance with Niehaves et al.:

Carrying out a content-analysis, Niehaves et al. discovered that most papers point to employee satisfaction as the most evident advantage of BYOD and security issues as the most evident disadvantage. Table 3 summarizes the risks incurred by BYOD (Clarke et al. 2012a). Yet, this analysis is based on the assumption that any given organization has implemented a BYOD policy. The x point to major effects, the (x) to side effects.

Table 2 Advantages and disadvantages of BYOD (based on Mitterlehner 2014, p. 219)

	Advantages	Disadvantages
Employee	• Autonomy • Competence	• Workload due to unlimited availability
Organization	• Employee satisfaction • Speed of adoption • Employee availability • Consumer focus • Employee investments	• Security issues • Support complexity (if organization pursues a BYOD policy) • Loss of process control • Performance concerns

As outlined below in Table 3, general risks concern malware, economic espionage, man-in-the-middle-attacks/network-sniffing, loss of devices, etc. (Stork et al. 2012). Compliance (e.g., negligence or the nonrespect or nonexistence of BYOD policies) may be the most important aspect when it comes to Cyber-Security. An effective risk mitigation strategy must accept the state-of-the-art. Therefore, it must take account of and address technical, legal, and regulatory aspects at the same time. Those variables overlap, and their scope differs in accordance with the situation addressed.

- Employment law (what about maximum work times; is it possible to force staff to participate in BYOD strategies, data protection, and privacy concerns) (Pollert 2014)
- Data protection law
- License and copyright matters (software licensing) (Arning et al. 2012)

Even if technological mobile device management methods may help cope with this trend, BYOD is not an entirely technical issue.

By way of example, organizations are obligated to ensure data security and secrecy of telecommunications (German Telecommunications Act: Art 109); German Data Protection Act: Art 9) under German law. In fact, there are three ways to deal with the use of private end-devices for professional purposes. Organizations may ignore the use of private end-devices or applications, prohibit and restrict it completely, or implement a BYOD code of conduct/policy. The different coping strategies are displayed in Fig. 2.

Exploring the legal implications of BYOD, the following examples shall be discussed:

- A knowledge worker holds a contract with a telecommunication service provider and uses their private end-device for professional purposes. Even if this is not important for the issue discussed here, it is worthwhile mentioning that and organization ought to pay some indemnification if knowledge workers use their devices or applications for professional purposes
- A knowledge worker stores professional data in public clouds (e.g. Dropbox) in order to access and process this information when out of office

Table 3 Potential risks inherent in BYOD (based on Mitterlehner 2014, p. 220f)

Risk	Category			Explanation
	Costs	Legal	Data	
Increased variety and complexity	x	(x)	(x)	+ Higher investments instead of cost reduction due to: - IT-management - Security: protection and compliance, inclusive of support of employees using their own devices - Need for continuous adaptation and revision of policies (e.g., opening network perimeter security)
Loss of device	x	(x)	(x)	+ Device replacement (who is informed thereof, who pays?) + Data recovery + Data loss (who will be notified thereof?)
Adaptation of existing IT-security infrastructure (only if business pursues a BYOD policy)	x		(x)	+ Investment into device-agnostic security architecture: - Introduction of end-to-end security that dynamically adapts to the characteristics of the user-owned device- Enhancement of existing security policies - Awareness-raising/-training and security education
Corporate governance and compliance control over employee-owned devices (only if business pursues a BYOD policy)	(x)	x	(x)	+Traceability and manageability of user actions on consumer IT components that are not owned by the businesses + Resolution of security incidents (difficulties if no access to all parts of the consumer IT component is granted) + Incident management (in the event of absence of managed SLA agreements with involved providers) + Compliance with data protection regulation through loss of individual privacy, business data, and data integrity
Enforcement of legal and regulatory provisions and compliance controls	(x)	x		+ Difficulty to enforce compliance in privately owned and operated devices: - End-user activities within different jurisdictions (e.g., use of cloud services, e.g., drop boxes) - Definition of sphere of influence regarding data and applications on the end-user devices

(*continued*)

Table 3 (continued)

Risk	Category			Explanation
	Costs	Legal	Data	
				(e.g., HR policies, legal scope, and context and claims of ownership on intellectual property) - Labor law: unofficial teleworking, working outside working hours
Distinction between corporate and personal data on employee-owned devices	(x)	x	x	+ Inability to distinguish between user and business data stored on consumer devices ➔ privacy risk + Litigation with employees
Uncontrolled use of consumerized services/ devices (e.g., cloud computing, social media, drop boxes, browser data, and software and applications installed or used in mobile devices)	(x)	x	(x)	+ Neglect of existing security policies + Transfer of business information outside the security domain (access by nonauthorized individuals) +Disclosure or loss of information as a result of sharing of devices (with family and friends) or when a malicious individual gains physical access to the device or through the use of an attack ➔ Hazards: no automatic access locks, no security protocols to protect data on the move (unsecured channels), and immaturity and heterogeneity of consumer device software (vulnerabilities, lack of robustness and stability of the devices, applications and services used)
Access by unknown users and unmanaged devices to enterprise networks	(x)	(x)	x	Network intrusion (as a result of opening up the security perimeter to accommodate consumerization) Data loss (also: privacy risk)
Inability to control security in application-rich mobile devices/ mobile devices being the target of attack for the acquisition of corporate data		(x)	x	+ Weak security controls in consumer devices and also in the functions available on those devices (such as location tracking, private mail, app-stores, etc.) ➔ Risk that attack vectors, such as malware, phishing, identity theft, human engineering, spoofing, and eavesdropping will become far more significant

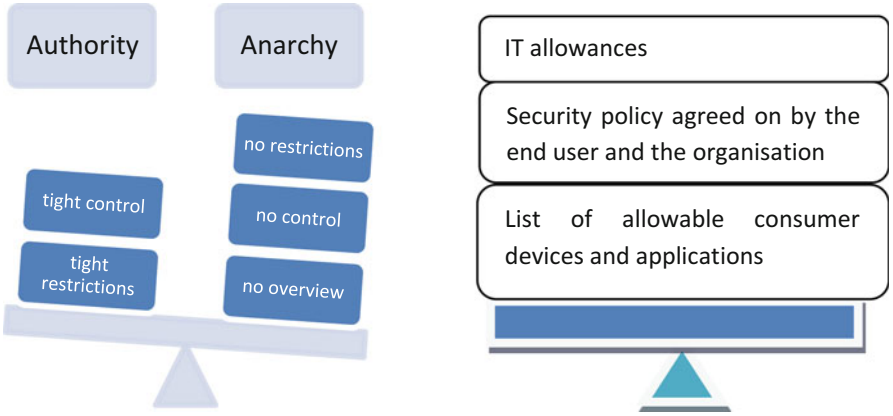


Fig. 2 Ways to deal with the use of private end-devices and applications in organizations, based on Mitterlehner (2014, p. 223)

The very first aspect which should not be neglected is that some service contracts are only available for private use. Those contract holders are, in fact, not allowed to use their end-devices for work purposes. Furthermore, the German labor court decided that the use of nonencrypted passwords cannot entail the immediate termination of a contract without notice if this has not been communicated beforehand (German Labor Court 2011). The respective organization would have to prohibit such actions beforehand. This also applies to the general use of private devices for work. Yet, organizations might prohibit the possession and usage of private applications and end-devices at work (German Works Constitution Act: Art. 87 para 1 [1]) without consulting the worker's council (if there is any) (German Labor Court 2009). There is no basic right to take one's ICT user applications or end-devices to the office and (even) use them there (German Labor Court 2009). Yet, since such a prohibition would undermine the benefits that can be created through work-flexibility, this solution might only be recommended for highly classified information. While the prohibition of the use of private smartphones for professional reasons seems feasible (even if unlikely), it proves extremely difficult to extend this prohibition to the whole Cyber-Space. It is of no use to block overall Internet access as the Internet has become a cornerstone of the knowledge worker's work. Given the amount of public cloud applications available and popping up on the Internet every day, it would become a never-ending story and impossible undertaking for the security IT department to search and block all of them (ENISA 2012).

Furthermore, data protection law and personal rights inhibit organizations from interfering with and controlling personal and private data on private end-devices (German Data Protection Act: Art. 32; Constitution of the Federal Republic of Germany: Art. 2). Consequently, organizations need the consent of their staff prior

to implementing any technical measures or regulations concerning data processing on private end-devices and applications. Without this, they may not store the privately exchanged, consumed, or downloaded data of the knowledge worker. One solution would be to create two user surfaces on the same device, and, concerning smartphones, to assign two different numbers to it (Clarke et al. 2012b).

Moreover, it is difficult for organizations to impose rules on their staff concerning the ways they use their private end-devices and different applications in their free time. In their leisure time, knowledge workers might choose apps in accordance with their taste and leisure time activities. If they install and use insecure apps, harmful content might make its way to the business network without being noticed by the firewall so that business data would be read and transmitted to third parties or the developer of the app (e.g., terms and conditions) (ENISA 2012, Clarke et al. 2012a). However, if knowledge workers were restricted in the private use of their (!) end-devices, BYOD would neither be fruitful for them nor the organization.

Labor law aspects also merit consideration. While the new paradigm of work-life flexibility dissolves the frontiers between private and professional life, labor laws impose maximum hour thresholds and minimum periods of leisure time between work (German Civil Code: Art 675; German Civil Code: Art 670). Even though BYOD fosters work-flexibility which is an integral characteristic of a knowledge worker's way of working, it may transform them into "slaves of their work".

Finally, cloud computing is an effect of CoIT, too, and was already mentioned in this chapter several times as BYOD and cloud computing often go hand in hand. There are different forms of cloud computing. It shall be referred to, for an increasing number of composite applications use components which are increasingly delivered via the cloud (facebook, apps, Dropbox). There are different levels of cloud computing: IaaS, PaaS, and SaaS. Yet, they all have in common one basic security risk: data loss. By way of example (ENISA 2012):

- Data location is not always identifiable (transparent) – be it in a public or in a private cloud. This is due to subcontracting and international contract law
- Strong dependence on the availability of infrastructure and networks
- No or insufficient distinction between or isolation of data processing (for the various users)
- Unauthorized access to data possible in case of misconfiguration
- Guarantee of confidentiality, security, or integrity of the data; liability in case of a breach thereof

As soon as information is put on a cloud, an attack from an external source will expose to the attacker all information stored on this cloud (= single point of failure) (ENISA 2009; 2012). The use of public cloud services for storing or processing business information entails a loss of knowledge control for organizations (Moore 2011). As knowledge workers take the lead and make their own IT decisions, IT departments may no longer control which kind of information remains within the organization (Harris et al. 2011; Price Waterhouse Coopers 2011).

A recent ENISA study showed that not even organizations bear in mind all security aspects that would have to be settled in service level agreements when outsourcing data to clouds (ENISA 2011). The probability that knowledge workers/employees know about these risks and attempt to avoid them when using their private end-devices or applications in their leisure time is likely to be even lower.

As it is difficult to completely restrict the use of private end-devices and applications (as already said, problem of non-respect and non-compliance), numerous papers recommend the implementation of BYOD strategies (Clarke et al. 2012a, b). Awareness created through BYOD strategies helps organizations to better control this trend, even if this does not definitely rule out any risks of nonproper handling of information, for it may never be excluded that compliance rules are disrespected.

Legal Implications

While the previous subchapter points to some specific legal issues, general challenges shall be pointed out in this subchapter.

As ICT use increases, our dependency on ICT and its availability (technology as a conditio sine qua non) increases, too. At the same time, developers and producers put security on the back burner and emphasize intuition and design. IT both amplifies and accelerates the momentum of knowledge democracy and establishes new qualities of public space and infrastructures which transcend the borders and boundaries of nation states and also extend towards a new territory – the Cyber-Space (Campbell 2014, p. 114). In a global society, it is no longer possible to control or suppress global flows of knowledge (Campbell 2014, p. 115). This (along with decreased security standards and negligence or lack of awareness) increases the dangers and negative impact attached to (e.g., infrastructural) attacks (examples include "Sasser" and "Stuxnet") as well as the number of (potential) victims (Gercke 2008). The Cyber-Space has, thus, come to challenge our legal framework, of common rights and freedoms. Campbell gives the examples of qualification of a letter compared to an e-mail and spying activities among governments (Campbell 2014, p. 114). This is also highlighted by Ullrich and Weippl stating that "Practically everbody's Internet communication is collected," whereby the actors who are after gaining, altering, analyzing, measuring, and finally storing data in order to generate a precise picture of Internet users include not only cyber-criminals but also public authorities and Western democracies and, of course, commercial enterprises (Ullrich and Weippl 2015, p. 448).

As a consequence, legal and regulatory issues need to be addressed besides sociopolitical or technical ones when it comes to "tackling the Cyber-Space". Legal sets define the framework within which Cyber-Democracies and knowledge societies flourish by setting the minimum conditions to safeguard security in our cyber-activities (Fig. 3).

As pointed out, "not everything, which is technically possible, is also feasible in terms of democracy and quality of democracy." According to Campbell, a need for restricting (technically possible) monitoring activities of democratic

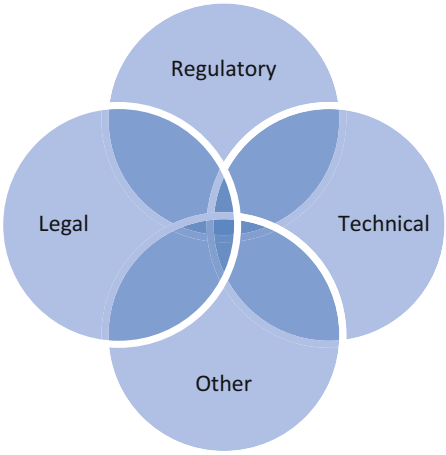


Fig. 3 Dimensions of Cyber-Management, based on Mitterlehner (2014, p. 222)

governments against their own citizens and residents (in the form of self-restrictions) ensues from that (Campbell 2014, p. 115). Unfortunately, law-making processes and decision-makers have waited too long to address this paradigm change. Legal systems (in Europe both supranational and national ones) popularly lag behind this plethora of technological developments of the past decades. The laws that exist are too tight and narrow and have not been adapted to the wide array of technological possibilities and uses (Klöpfer and Neun 2000). Given all this, regulation has taken place on soft law and bottom-up levels via compliance, voluntary sets of rules, and voluntary regulation (standards, codes of conduct, etc.) (Klöpfer and Neun 2000).

Indeed, it is a difficult undertaking to start with, since it seems unclear where to start. One idea would be to begin with the most serious cases in order to counterfight Cyber-Crime and then to turn to the ones with a lesser impact. The concept of Cyber-Crime alone is a concept as vast as the one of Cyber-Space. It comprises:

- Copyright infringements
- Pornographic, politically extremist, or violent multimedia content
- Introductions to violence and crime (e.g. How to make bombs [Gercke 2008]: Thanks to the Internet, this kind of information may be retrieved in an easier, faster, and more anonymous way. Services such as Google Earth and Google Maps make it easier to learn about potential targets of attacks.)
- Illegal traffic (inclusive of illegal currencies)
- Data protection infringements, spying, hacking
- Terrorism, attacks on ICT-controlled infrastructure
- Digital identities and theft of identities (Hansen and Meissner 2007)
- Automatized attacks (e.g., Denial-of-Service attacks, Botnetworks); see Gercke 2008: On average, every computer is attacked for the first time already after 39 s after starting it

Yet, the Cyber-Space must not be seen as a legal space detached from the real world which needs its own rule. Any such views represent "cyber-romanticism at its worst." Instead, the same sets of laws need to apply to the real and the virtual world (Shapiro 1998).

The insufficient legal framework is only partly due to the quick technologization and failure to respond in time. It is worthwhile to mention that any challenges we are facing now partly originate from the very beginning of the cyber-age, as the Internet was developed without the influence of a state or a sovereign. Likewise, technological standards were set by private and voluntary committees such as the *Internet Engineering Task Force* IETF or ICANN which administers DNS. Only slowly would this form of governance be questioned (Vögeli-Wenzl 2007). While the lack of state regulation might have been essential for the Internet to develop as dynamically as it did, its inherent drawback is that it is barely possible to govern or control such a free, anarchical development. As the spheres of law and economy have been lifted to another (decentralized, global) level it becomes even more difficult to introduce measures of governance and control.

Challenges which slowly start to be seen do not necessarily entail a legal vacuum, though. Still, self-regulation and private players are no panacea to all the challenges attached to new media, services, and devices, but a remedy (Klöpfer and Neun 2000). The major challenges to combat Cyber-Crime concern: (Gercke 2008)

1. Questions of logistics (Cyber-Crimes can be controlled and stirred from any place)
2. Localization and tracking
3. Competences, in particular with regard to international penal dimensions and cooperation; take for instance "Love Bug" and the difficulties in penal prosecution as a result of Philippine laws
4. In combination with point 2: The limited impact of counter-measures; it is not sufficient to implement national blockings as illegal content may be distributed via other channels and, this in combination with the limited applicability of national penal law and the international principle of sovereignty makes it difficult for law-enforcing authorities to act (art 7 para 2 Telemediengesetz (Telemedia Act) provides the legal foundation for block orders in Germany.)
5. The vastness of the Internet (filters and keyword-based search functions are not entirely successful to track down contents or persons)
6. The anonymosity of the Internet (public access, anonymization servers, open wireless networks, hacking of private wireless networks, prepaid mobile cards)
7. Network resilience against external controls (see Gercke 2008: As the Internet builds on an architecture developed for military purposes, essential control instruments are lacking.)
8. The limited applicability of potentially successful investigation measures (data storage, online searches) due to potential interventions with the law or fundamental rights. There are two sides to the medal when it comes to data deletion: The right to be forgotten and privacy protection are obstacles to cyber-governance and data tracking

Therefore, Cyber-Governance is a key issue (Eriksson and Giacomello 2006), notably when it comes to questions of how to protect states, organizations, and citizens without depriving them or anybody else of their (freedom) rights (e.g., expression of opinion).

Since the self-regulating force of the Internet cannot meet its inherent challenges, penal governance needs to be enforced, whereby it takes a minimum level of control (which cannot be imposed at national level only) and laws or other means of regulation. International measures and close cooperation in cases of transnational Cyber-Crime are crucial. If solely imposed at national level, criminals will turn to countries, where they will not be prosecuted and launch their actions from there. So far, this is governed by agreements on mutual assistance; requests for mutual assistance are lengthy and complicated, though. Furthermore, measures are difficult to adopt since they comprise a wide array of different legal areas, such as:

- Penal law
- (Civil) contract law, consumer protection law
- Industrial property rights (copyright, trademarks, patents)
- Competition law (fair practices, antitrust law)
- Data protection and trade secrets
- Telecommunication law
- Media law

Conclusion

The emergence of the Cyber-Space in its present form has its origins in the Consumerization of IT. The latter has led to the democratization of IT by providing individuals with very powerful ICT and granting access to an infinite Cyber-Space. The relatively new, multifaceted opportunities of the Cyber-Space endorse knowledge dissemination and may endorse democracy or even lift it to another level. Not only may the Cyber-Space be used to revive political interest and participation, but also it may raise transparency and awareness about political questions and issues at stake among the general public. In particular, Web 2.0 has increased the potential for democratic citizenship. As such, civil society may come to stir and participate in the decision-making processes and agenda-setting when it comes to issues which used to be left to the heads of states and governments. Consequently, the Cyber-Space is a strong instrument to promote global democracy and global networks by adding weight to bottom-up movements and foster knowledge democracy. It may also further global awareness and transnational democracy.

While CoIT has paved the way for the general public to engage in cyber-citizenship, it is difficult to assess if Cyber-Democracy will have a tangible effect in terms of electoral suffrage, though. Therefore, a wide definition of cyber-democratic action/participation needs to be applied, extending the typical definitions of e-democracy and construing it as a form of knowledge democracy. Such a wide concept of democratic citizenship goes beyond electoral suffrage and includes

expressions of disappointment, mistrust, and disillusionment. The Cyber-Space has spurred their impact as it communicates them at global level. Since the Internet has become a fundamental service in industrialized nations, its impact on democracy and agenda-setting should definitely be observed more closely, emphasizing also expressions of discontent and bottom-up mobilization.

Yet, the Cyber-Space being a new decentralized communication and action platform also provokes (new forms of) criminal activities which are often difficult to classify and distinguish from transparency measures, awareness-raising, civil empowerment, and Cyber-Crime (e.g. criminal acts of disclosure affecting businesses providing fundamental services or national security). This particularly applies to hacktivism – as carried out by Anonymous – which is governed by a sort of ethical code. Also, Bring-Your-Own-Device (BYOD) is a recent trend which illustrates this very well. On the one hand, powerful commercialized ICT gives the general public the opportunity to engage in democratic citizenship by seeking, sharing, and creating information at any place and time. On the other hand, the use of professional information on private end-devices or applications represents a security risk for organizations, for private end-devices may be less secure, stolen, or lost and public applications be hacked or information on those applications shared with third parties without even knowing. Potential risks associated to BYOD may affect society at large. This is particularly so if attacks concern national authorities or public utilities. While there are technical solutions to avoid this, just as the creation of two user surfaces on the same device or the assignment of two different numbers to one single smartphone, such measures may not be implemented without the consent of the private owner of the device (the employee). Also, even if it is valid for an organization to completely prohibit the use of private end-devices and public applications at work this definitely constitutes an infringement of one's freedom of expression and, from an economic point of view, may interfere with the creative potential of the knowledge worker. Cloud solutions will not cease to be used as they prove highly efficient when it comes to the storage of large data volumes (e.g. for camera records, etc.). Therefore, compliance is at the very heart of risk mitigation strategies.

In conclusion, the Cyber-Space and ICT have added a new dimension to our society and brought about a global (knowledge) society. As this entails chances and challenges, Cyber-Governance is needed. This paper presents an overview of the democratic potential of the Cyber-Space while pointing to the flipside of the coin, notably for businesses, but also the sovereign. Consequently, it is necessary to bear in mind the consequences of CoIT. The general public (and, thus, the knowledge worker) will not cease to possess powerful ICT. On the one hand, this may represent a considerable security risk. On the other hand, it may further the creative potential of citizens and bring about new methods of agenda-setting.

The major challenges to combat Cyber-Crime comprise questions in the field of logistics, localization and tracking, transnational cooperation, anonymity, network resilience, data protection (which can hinder investigation), etc. Our sets of laws and regulatory frameworks need to be updated and amended in order to take account of this new e-dimension and the risks attached to it, for even if technological management methods may help cope with the existing challenges to some degree, this is not a

purely technical issue but a key paradigm change within our society. We need rules that address Employment law; Data protection law; Penal law; (Civil) contract law; Consumer protection law; Industrial property rights (copyright, trademarks, patents, license matters); Competition law (fair practices, antitrust law); Telecommunication law; Media law, etc. Already from the mere number of rules needed it can be deducted which far-reaching repercussions the Cyber-Space has had in and on our society. Being such a wide field of action, it definitely needs to be evaluated more closely.

References

Aerospace Industries Association. (2011). *Best practices for exploiting the consumerization of information technologies*. Arlington.

Andriole, S. J. (2012). Managing Technology in a 2.0 World. *IT Professional, 14*(1), 50–57.

Arning, M., Moos, F., & Becker, M. (2012). Vertragliche Absicherung von Bring Your Own Device. *Computer und Recht, 28*(9), 592.

Barber, B. R. (1999). Three scenarios for the future of technology and strong democracy. *Political Science Quarterly, 113*(4), 573–589.

Baron, N. S. (2008). *Always on: Language in an online and mobile world*. Oxford: Oxford University Press.

Baskerville, R. (2011). Individual information systems as a research arena. *European Journal of Information Systems, 20*, 251–254.

Benton Foundation. (1998). *Losing ground bit by bit: Low-income communities in the Information Age*. Washington, D.C.: Benton Foundation and National Urban League. In. http://www.eric.ed.gov/PDFS/ED424333.pdf.

Betriebsverfassungsgesetz. (2001). (BetrVG) as of 25 September Federal Gazette BGBl. I. pp. 2518. Last amendment as of 20 April 2013. Federal Gazette BGBl. I. pp. 868).

Brandtzæg, P. B., & Heim, J. (2009). Why people use social network sites. In *Online communities* (pp. 143–152). Berlin: Springer.

Bundesdatenschutzgesetz. (2003). (BDSG) as of 14 January Federal Gazette BGBl. I. pp. 66. Last amendment as of 14 August 2009. Federal Gazette BGBl. I. pp. 2814.

Bundesrepublik Deutschland. (2004). Telekommunikationsgesetz (TKG) as of 22 June. Federal Gazette BGBl. I. pp. 1190. Last amendment as of 3 May 2012. Federal Gazette BGBl. I. pp. 958–1717.

Bürgerliches Gesetzbuch. (2002). as of 2 January Federal Gazette BGBl. I. pp. 42, 2909. Last amendment as of 7 May 2013. Federal Gazette BGBl. I. pp. 1122.

Campbell, D. F. J. (2014). Cyber-democracy. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 114–116). New York: Springer.

Campbell, D. F. J., & Barth, T. D. (2009). Wie können Demokratie und Demokratiequalität gemessen werden? Modelle, Demokratie-Indices und Länderbeispiele im globalen Vergleich. *SWS-Rundschau, 49*(2), 208–233.

Campbell, D. F. J., & Carayannis Elias, G. (2014). Explaining and comparing quality of democracy in quadruple helix structures: The quality of democracy in the United States and in Austria, challenges and opportunities for development epilogue on cyberdemocracy. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 118–146). New York: Springer.

Campbell, D. F. J., Carayannis Elias, G., & Rehman, S. S. (2015). Quadruple Helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493.

Carayannis, E. G., & Campbell, D. F. J. (2009). "Mode 3" and "Quadruple Helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46* (3/4), 201–234.

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple Helix, Quadruple Helix and Quintuple Helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69. In: http://www.igi-global.com/bookstore/article.aspx?titleid=41959.

Carayannis, E. G., Barth, T. D., & Campbell, D. F. J. (2012). The Quintuple Helix innovation model: Global warming as a challenge and driver for innovation. *Journal of Innovation and Entrepreneurship, 1*(2). In: http://www.innovation-entrepreneurship.com/content/1/1/2.

Castells, M., & Cardoso, G. (2005). *The network society. From knowledge to policy.* Washington, DC: Johns Hopkins Center for Transatlantic Relations.

Cavelty, M. D. (2012). Cyber(Un)Sicherheit: Grundlagen, Trends und Herausforderungen. *Politische Bildung, 1*, 66–87.

Charter on the Fundamental Rights of the European Union. 2000/C 364/01.

Chen, W., & Wellman, B. (2005). *Minding the cyber-gap: The Internet and social inequality*, *The Blackwell companion to social inequalities*. Oxford: Blackwell Publishing.

Chiarella, D. J. G. (2013). *Inside anonymous hacker group. A special report to the FBI Baltimore office*. Lulu Press.

Choucri, N. (2000). Introduction: CyberPolitics in international relations. *International Political Science Review, 21*(3), 243–263.

Clarke, J., Hidalgo, M. G., Lioy, A., Petkovic, M., Vishik, C. & Ward, J. (2012a). Consumerization of IT: Risk mitigation strategies, ENISA.

Clarke, J., Hidalgo, M. G., Lioy, A., Petkovic, M., Vishik, C., & Ward, J. (2012b). Consumerization of IT: Top risks and opportunities. Responding to the Evolving Threat Environment, ENISA.

Coleman, S., & Blumler, J. (2009). *The Internet and democratic citizenship: Theory, practice and policy.* Cambridge: Cambridge University Press.

Collins, D. (2001). *Carrier grade voice over IP.* New York: McGraw-Hill.

Coopers, P. W. (2011). *The consumerization of IT - The next generation CIO*. New York: Center for Technology and Innovation.

Dahlgren, P. (2003). *Reconfiguring civic culture in the new media milieu. Media and the restyling of politics: consumerism, celebrity, cynicism* (pp. 151–170). London: Sage Publications.

Digitales Österreich. (2012). Nationale IKT-Sicherheitsstrategie Österreich.

DiMaggio, P. & Hargittai, E. (2001). From the 'Digital Divide' to 'Digital Inequality': Studying Internet use as penetration increases. Working Chapter 15, Summer 2001, Center for Arts and Cultural Policy Studies, Princeton University.

DiMaggio, P., Hargittai, E., Celeste, C., & Shafer, S. (2004). Digital inequality: From unequal access to differentiated use. In *Social inequality.* New York: Russel Sage Foundation.

Drury, A. & Absalom, R.. (2012). *BYOD: An emerging market trend in more ways than one*. White Chapter, Ovum, Logicalis Group.

ENISA. (2009). Cloud Computing. Benefits, risks and recommendations for information security.

ENISA. (2011). Survey and analysis of security parameters in cloud SLAs across the European public sector.

ENISA. (2012). Critical Cloud Computing. A CIIP perspective on cloud computing services. Version 1,0.

Entity Solutions. (2013). The workforce of the future embraces flexibility for knowledge workers. Blog, posted date: January 9, 2013. In: http://blog.entitysolutions.com.au/the-workforce-of-the-future-embraces-flexibility-for-knowledge-workers/.

Eriksson, J., & Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? *International Political Science Review/Revue internationale de science politique, 27*(3), 221–244. Sage Publications.

Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation: From National Systems and "Mode 2" to a Triple Helix of university-industry-government relations. *Research Policy, 29*, 109–123.

European Commission. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Agenda for Europe. COM/2010/0245.
Eurostat. (2013). Haushalte, die Zugang zum Internet haben, nach Art der Verbindung.
Friedman, T. L. (1999). *The Lexus and the Olive Tree: Understanding globalization*. New York: Random House.
Gercke, M. (2008). Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden, MMR , pp. 291–298.
German Labor Court Ludwigshafen. (2009). Judgment of 30 October 2009. Case 6 TaBV 33/09.
German Labor Court Nürnberg. (2011). Judgment of 24 March 2011. Case AZR 282/10.
Gibbons, M., Limoges, C, Nowotny, H, Schwartzman, S, Scott, P, & Trow, M (1994). *The new production of knowledge*. The dynamics of science and research in contemporary societies. London: Sage.
Gilbert, J. (2012). Tech Trends. Bring Your Own Device to Work. Lexicon Systems. In: http://www.lexicon-systems.com/pubs/itinsight/ITInsight1208.pdf; http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6017170&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6017170.
Goodrum, A., & Manion, M. (2000). Terrorism or civil disobedience: toward a hacktivist ethic. *Computers and Society, 30*(2), 14–19.
Goodrum, A., & Manion, M. (2007). Terrorism or civil disobedience: toward a hacktivist ethic. In K. E. Himma (Ed.), *Internet security. Hacking, counterhacking, and society* (1st ed., pp. 61–72). Jones and Bartlett Publishers.
Grundgesetz für die Bundesrepublik Deutschland. (2012). Last amendment as of 11 July. Federal Gazette BGBl. I. pp. 1478ff.
Hai-Jew, S.: Action potentials (2013). Extrapolating an ideology from the Anonymous Hacker Socio-Political Movement (A qualitative meta-analysis). Kansas State University, Manhattan, 2013, 51–107. In: Acricopoulou, Christina, Garipidis, Nicolaos: *Digital democracy and the Impact of technology on governance and politics: New globalized practices*., Information Science Reference, USA.
Halavias, A. (2009). *Search engine society.* Cambridge: Polity.
Hammond, A. L. (2001). *Digitally empowered development*. Council of Foreign Relations: Foreign Affairs.
Hansen, M., & Meissner, S. (2007). *Verkettung digitaler Identitäten* (1st ed.). Schleswig-Holstein: Unabhängiges Landeszentrum für Datenschutz.
Harris, J. G., Ives, B., & Jungla, I. (2011). The Genie Is Out of the Bottle: Managing the Infiltration of Consumer IT Into the Workforce. Accenture Institute for High Performance. In: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Managing-the-infiltration-of-Consumer-IT-into-the-workforce.pdf.
Heckmann, D. (2011). Open Government – Retooling Democracy for the 21st Century. 44th Hawai International Conference on Systems Sciences (HICSS).
Himma, K. E. (2007). Hacking as a politically motivated digital civil disobediance. Is hacktivism morally justified? In K. E. Himma (Ed.), *Internet security. Hacking, counterhacking, and society* (1st ed., pp. 73–98). Jones and Bartlett Publishers.
Infosecurity Magazine. (2012). Crystal ball time: Top 2013 risks include cyber war, cloud and BYOD.
International Standards Organisation. (2011). ISO/IEC 27005.
International Telecommunication Unions. (2008). Series X: Data networks, open system communications and security. Telecommunication security. Overview of. Recommendation ITU-T X.1205. 04/2008.
Kaneshige, T. (2012). BYOD - Five hidden costs to a bring-your-own-device progamme. Computerworld UK – The Voice of IT Management.
Karamagioli, E. (2013). Transparency in the open government era: Friends or foes. In C. Acricopoulou & N. Garipidis (Eds.), *Digital democracy and the impact of technology on governance and politics: New globalized practices*. Paris: Paris 8 University. Information Science Reference, USA.

Klein, A., Vöhringer, B., Krcmar, H. (1999). Cyberdemocracy – Neue Chance für Demokratie? In: http://www.winfobase.de/lehrstuhl/publikat.nsf/intern01/076790EF7CDE06A84125686C002CCFCD/$FILE/99-19.pdf.

Klöpfer, M., & Neun, A. (2000). Rechtsfragen der europäischen Informationsgesellschaft, EuR 2000, 512ff.

Kompetenzzentrum Internetgesellschaft. (2013). Geschäftsstelle Rundfunk und Telekom Regulierungs - GmbH, (ed.). Stand IKT in Österreich, 1. Bericht des Kompetenzzentrum Internetgesellschaft.

Leigh, D. & Harding, L. (2011). WikiLeaks. Inside Julian Assange's war on secrecy. The Guardian.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (1997). *A brief history of the Internet*. Internet Society. In: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Leiner.

Lennon, R. G. (2012). Bring your own device (BYOD) with Cloud 4 education. Letterkenny Institute of Technology. In Splash '12: Proceedings of the 3rd annual conference on Systems, programming, and applications: software for humanity. New York. pp. 171–180.

Livingstone, S., Ólafsson, K., & Staksrud, E. (2011). *Social networking, age and privacy*. London: EU Kids Online. http://eprints.lse.ac.uk/35849/1/Social%20networking%2C%20age%20and%20privacy%20%28LSERO.pdf.

Loader, B. D., & Mercea, D. (2011). INTRODUCTION NETWORKING DEMOCRACY? Social media innovations and participatory politics. *Information, Communication & Society, 14*(6), 757–769.

Maier, R., Thahmann, S., Bayer, F., Krüger, M., Nitz, H., & Sandow, A. (2008). Flexible office: Assignment of office space to enhance knowledge work productivity. *Journal of Universal Computer Science, 14*(4), 508–525.

Markopoulou, A.P., Tobagi, F. A., & Karam, M. J. (2002). Assessment of VoIP quality over Internet backbones, *1*, 150–159.

Markopoulou, A. P., Tobagi, F. A., & Karam, M. J. (2003). A. P. (2003). Assessing the quality of voice communications over internet backbones. *IEEEACM Transactions on Networking, 11*(5), 747–760.

Martinez, E. & Rajlkashmi, S. (2012).Workplace 2030 Workplace 2030. People Matters. In: http://www.peoplematters.in/articles/focus-areas-13/what-is-hot/workplace-2030.

Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology. U.S. Department of Commerce. In: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Mitterlehner, B. (2013). Daseinsvorsorge als europäischer Begriff. In: Der europäische Antagonismus – Binnenmarkt und Daseinsvorsorge. Schriftenreihe Daseinsvorsorge Vol 1. Public Social Responsibility Institut.

Mitterlehner, B. (2014). Cyber-democracy and cybercrime: Two sides of the same coin. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 207–230). New York/Heidelberg/Dordrecht/London: Springer.

Mitterlehner, B. & Barth, T. D. (2013). Daseinsvorsorge: Grundaufgabe und Begriff. In: Der europäische Antagonismus – Binnenmarkt und Daseinsvorsorge. Schriftenreihe Daseinsvorsorge Vol 1. Public Social Responsibility Institut.

Moore, G. (2011). *Systems of engagement and the future of enterprise IT- A sea change in enterprise IT*. Silver Spring: AIIM.

Moschella, D., Neal, D., Opperman, P., & Taylor, J. (2004). *The "Consumerization" of Information Technology*. El Segundo: CSC. http://www.smaele.nl/edocs/Taylor-Consumerization-2004.pdf.

Murdoch, R., Harris, J. G. & Devore, G. (2010). Can Enterprise IT Survive the Meteor of Consumer Technology? Accenture Institute for High Performance. In: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture_Can_Enterprise_IT_Survive_the_Meteor.pdf

Niehaves, B., Köffer, S., Ortbach, K. & Katschewitz, S. (2012). Towards an IT Consumerization Theory - A Theory and Practice Review. In: Working Chapters, European Research Center for Information Systems No. 13. Eds.: Becker, J. et al. Münster. July 2012.

Nye, J. S. (2010). *Cyber power*. Belfer Center for Science and International Affairs: Havard Kennedy School.
Olsen, R. K. (2009). The DemoCratic Workplace. Empowering People (demos) to Rule (cratos) their own workplace. Organizing Individual and Group Decision Processes through Personal Competence-based Authority.
Oppliger, R. (2011). Security and Privacy in an Online World. In: IEEE Computer. Vol 44, Issue 9.
Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age*. Cambridge: Polity.
Pollert, D. (2014). Arbeitnehmer-Smartphone als Betriebsmittel – ein kostensparendes Modell? NZA-Beilage , pp. 152–155.
Poster, M. (1995). *Cyber democracy: Internet and the public sphere*. Irvine: University of California. http://www.hnet.uci.edu/mposter/writings/democ.html.
Poster, M. (2001). What's the Matter with the Internet, Electronic Mediations Vol. 3, Minnesota.
Rettberg, J. W. (2008). *Blogging*. Cambridge: Polity Press.
Rose, C. (2013). BYOD: An Examination of Bring Your Own Device in Business. Review of Business Information Systems – Second Quarter 2013. Vol 17 (2). The Clute Institute. In.
Sambharya, R. B., Kumaraswamy, A., & Banerjee, S. (2005). Information technologies and the future of the multinational enterprise. *Journal of International Management, 11*(2), 143–161.
Schaffry, A. (2013). *Security, Kosten und Verwaltung. Die größten Probleme bei BYOD*. Munich: CIO, IDG Business Media GmbH.
Squires, J. (1998). In different voices: Deliberative democracy and aestheticist politics. In *The politics of postmodernity* (pp. 126–146). Cambridge: Cambridge University Press.
Stork, J., Steup, S., & Satschek, P. (2012). Betrachtung sicherheitsrelevanter Aspekte zur Nutzung privater ITK im Rahmen des "Bring your own Device" Konzeptes. Hochschule für Oekonomie & Management. Duisburg. 13 July 2012.
Telemediengesetz. (2007). (Telemedia Act) of 26 February . Federal Gazette I p. 179), last amendedment: 17 July 2015.
Treaty on European Union. (2012). Consolidated version. Official Journal of 26 October 2012, C 326, pp 13ff.
Treaty on the Functioning of the European Union. (2012). Consolidated version. Official Journal of 26 October 2012, C 326, pp 47ff.
Voegeli-Wenzl, J. Internet Governance am Beispiel der Internet Corporation of Assigned Names and Numbers (ICANN), GRUR Int 2007. pp. 807–816.
Williams, R. W. (2006). Democracy, cyberspace, and the body, 2006. http://clogic.eserver.org/2006/williams.html
Xavier, R. F., & Campbell, D. F. J. (2014). The effects of cyberdemocracy on the Middle East: Egypt and Iran. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 147–173). New York/Heidelberg/Dordrecht/London: Springer.

Crowdsourcing Social Innovation: Toward a Collaborative Social Capitalism

29

Emanuele Musa

Contents

Babele (www.babele.co) is an open-innovation and mentoring network to help social innovators refine their business model through crowdsourcing. It is a powerful tool for cohorts of entrepreneurs, for peer-learning as well as community engagement and online mentoring.

E. Musa (✉)
Babele, Roumania, Italy
e-mail: manu@babele.co

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_2

Abstract

The growing awareness of humanity's finite resources and recognition of the limitations of one-off projects are prompting step changes in development planning. Sustainable development addresses the limitations of current practices; its aim is to achieve the triple bottom line of economic prosperity, environmental quality, and social equity, meeting the needs of present society without compromising resources for future generations.

Collective intelligence is considered by both Charles Leadbeater (former advisor to Tony Blair) and MIT as one of the most powerful ways to tackle complex problems, like climate change.

This chapter explores the principles of crowdsourcing, its applications, and the main trends. It presents theories, practices, and examples of the use of crowdsourcing to innovate in the area of sustainable development for the common good. It announces the rise of collective brain-power to the challenge of creating better and more effective forms of civic and social engagement to solve problems on a world scale.

Keywords

Crowdsourcing · Open innovation · Collaboration · Sustainability · Social innovation · Lean startup · Participatory democracy · Stakeholder participation

Introduction

The growing awareness of humanity's finite resources and recognition of the limitations of one-off projects are prompting step changes in development planning. Sustainable development addresses the limitations of current practices and features at the center of almost every political, environmental, scientific, and economic discussion held today. Its aim is to achieve the triple bottom line of economic prosperity, environmental quality and social equity, and meeting the needs of present society without compromising resources for future generations.

The 1992 Rio Earth Summit was the moment when sustainable development captured worldwide attention. It established why sustainable development is necessary; the project now is how to execute it. The twenty-first century is the era of mass innovation – more ideas, knowledge, and information being shared by more people than ever before. Can we harness collective brainpower to innovate in the area of sustainable development for the common good? Google, Wikipedia, and Linux are already using collective intelligence to develop new solutions through online communities. Could a collaborative online approach do the same for sustainable development?

- The participation, investment, and inclusion of all members of society in the development process is the key to not only help people fulfill their human potential, but also to ensure that a new model of democracy is established, which is capable of responding more effectively to the most urgent challenges of our time.

The Limits of Capitalism

At the beginning of the twenty-first century, the world seems more divided than ever.

The world GDP keeps growing year after year, so, in theory, we are all getting wealthier. However, the gap between the richest and the poorest is increasing and the richest 1% of the population will soon possess half of the global wealth. We keep extracting, exploiting, and consuming at a rate that was never so high before. We are increasingly pollution, despite the evidence of global warming, the alarming loss of biodiversity, and the uncountable number of lives wasted throughout the process to consumerism.

A "revolution" toward a large-scale improvement of well-being and sustainable development is approaching.

The growing awareness of humanity's finite resources and the impossibility to achieve an infinite economic growth in a finite planet are demonstrating the incapability of the capitalistic model to reduce inequalities and address the most urgent challenges of our time.

Although market forces demonstrated to be a nonsufficient mean to lead to the most efficient allocation of resources, governments, and institutions have failed to meet the needs of the Common Good and bring society together to solve global issues:

- Every year, nearly 12 million children die of mainly preventable causes, including diseases for which vaccines are routinely administered in many countries.
- Although access to safe drinking water increased from 61% in 1990 to 71% by mid-decade, 1.4 billion people in developing countries still lack such access. Furthermore, 2.7 billion people still do not have adequate access to sanitation.
- In the developing world, about 130 million children still remain out of primary school, nearly 60% of them girls. Adult illiteracy remains high, affecting roughly 855 million people, nearly two thirds of them women.
- According to the World Bank, in 2011, 17% of people in the developing world lived at or below $1.25 a day.

Through intense pressure from commercial marketing, **consumption** became the desire for status and social distinction at the personal and group level. Considering the finite natural resources available, it would be impossible for the estimated 2.2 billion people currently living on less than $2 a day to ever match the consumption level of the richest group. If every person on earth would consume at the same rate of a US citizen, we would need five planets to accommodate the need for resources.

We are still using a **linear system** applied to a **finite planet.**

Increases in poverty and inequality and the decline in opportunities have had a serious adverse effect on the well-being of individuals, communities, and even countries. Several critics have argued that the development orchestrated by the industrialized countries tended to replicate the forces of colonialism, continuing the pattern of resource expropriation and economic control by the industrialized countries.

The paradox of a global economy increasingly unified, and a global society increasingly divided is the most dangerous threat that weighs on the planet, because it makes the cooperation necessary to solve the most urgent problems of our time difficult, if not impossible.

What Is the Role of Business in Society?

To understand the role of business in society, we should go back a few centuries.

Until the seventeenth century, people owned businesses or worked for businesses, but they were just people, as the businesses did not exist independently of the people who owned them – thus, their individual ethics were directly reflected on these businesses.

When the first corporations came into existence, they were granted charters for specific short-term projects, like building a bridge or a railroad. Once they fulfilled their purpose, they were disbanded.

But over time, the law changed and corporations no longer had to be turned off once their project was complete. They began to live on indefinitely, with a much more general purpose: profit (Korten 2001).

Unlike people, who are driven by all kinds of motivations (doing the right thing, love for family, peers, the planet), publicly traded corporations are now required, by law and the markets, to maximize value for their shareholders, making as much profit as possible (Leonard 2007a, b).

The idea that a corporation's purpose is to maximize financial gain for its shareholders was first articulated in Dodge v. Ford Motor Company in 1919: Dodge v. Ford Motor Co. – 170 N.W. 668 (Mich, 1919). Over time, through both law and custom, the concept of "shareholder primacy" has come to be widely accepted. With such definition, there will always be a trade-off to be made between profits and the general interest of society.

Thus, there are many reasons why **the traditional business sector cannot become the drive behind substantial change**. If we have a look at the current situation throughout the world, we see a business environment that is shaped by a history of unhealthy competition, manifold cases of adulteration for the sake of profit, or the ongoing issues of child labor for the sake of reducing labor costs (Bakan 2004).

Reports about the horrible working conditions in the factories producing our iPads (Duhigg and Baraboza 2012) or the toxic chemicals contained in our everyday products are easily available. These examples show quite well how the drive for higher dividends is heavily corrupting the social sense of entrepreneurs.

Another false myth of liberal thinkers is the capability of the market to automatically adjust itself according to a continuously changing environment. For example, *when the issue of global warming will become an absolute priority, then the market will invest in greener technology that will take our CO2 emissions down*. The counter argument is that the planet does not respond to such linear thinking. Transgressing one or more planetary boundaries may be deleterious or even

catastrophic because of the risk of crossing thresholds that will trigger nonlinear, abrupt environmental change within continental- to planetary-scale systems.

Thus, even if we would drastically reduce our environmental impact, this would not bring us back to the same environmental conditions of the seventeenth century.

The short-term logic of the capital market is undermining our capability as a society to foster common good initiatives. The urgent environmental problems, and the incapability of this type of democracy, and of the market alone to handle them, request a totally fresh approach.

The New Way

Common good is broadly understood as the overall social condition that enables individuals or groups to attain their fulfillment more easily. Unlike the utilitarian approach, which focuses on the greatest good for the greatest number, the principle of the common good is geared toward the benefit of all (Paul 1991). As a reaction of the public institutions' failures to answer to the global need of common good, citizens are getting "smarter," more capable of interpreting issues and discerning between options on their own than simply accepting the views of media and political elites. In the global environment, several companies have come under pressure from civil society and nongovernmental organizations (NGOs) to be more responsive to the range of social needs in developing countries, including addressing concerns about the working conditions in factories or service centers, and attending to the environmental impacts of their activities.

Companies are an essential element of our society as they are deeply involved in the creation (or destruction) of common good, by providing workplaces adherent to law, ethical standards, and international norms. Their importance has increased over the last century to a point in which 52 of the 100 biggest economies on earth are now corporations (Anderson and Cavanagh 2005).

Thus, for society to thrive, it is fundamental that companies embrace responsibility for the impact of their activities on the environment, consumers, employees, communities, stakeholders, and all other members of the public sphere.

Today's corporate literature envisage a new economy that puts safe products, happy people, and a healthy planet first, where businesses proactively promote the public interest by encouraging community growth and development, and voluntarily eliminating practices that harm the public sphere, regardless of legality.

Can we review the way we create companies and measure success beyond profit? The key enabler for this new economy is **sustainable development,** which addresses the limitations of current business practices and promotes the deliberate inclusion of public interest into corporate decision-making. Its aim is to achieve the triple bottom line of economic prosperity, environmental quality, and social equity, meeting the needs of present society without compromising resources for future generations.

The 1992 Rio Earth Summit was the moment when sustainable development captured worldwide attention. It established why sustainable development is necessary; the project now is how to embed its principles in the market.

A New Business Sector

Typically, when we think about "sustainable business," we concentrate on corporate social responsibility (CSR): energy efficiency, reduced carbon footprint, recycling and reuse, fair treatment of employees, and charitable giving, among other considerations.

However, there is a growing market of mission-driven companies that are dedicated to being socially responsible from their inception, unlike most (though not all) corporations that pursue CSR for marketing purposes or to cut costs and increase profits.

The realm in which these mission-driven enterprises operate has come to be known as "social entrepreneurship," a term widely credited to Bill Drayton, founder of the social venture philanthropy, Ashoka.

Although the term "social entrepreneurship" is relatively new, initiatives to promote positive social change are not new. In fact, the earliest writings extend back to the late 1990s (Emerson and Twersky 1996). For example, the Greystone Bakery was founded in 1982 by Roshi Bernie Glassman, with the explicit mission to train and hire unemployed local residents, who otherwise would have struggled to obtain employment elsewhere. The Grameen Bank was founded in 1983 to provide rural illiterate women with access to microcredit facilities to launch new businesses.

"**Every time I see a problem, I create a business to solve it,**" says Professor Mohammed Yunus, the founder of the Grameen Bank, in his books. He describes social enterprises as businesses designed to meet a social goal, **not to create profit for its owners**.

The strength of being a social enterprise lies partly on its predisposition to bring lessons from business and apply them to answering social need. They bring the self-sufficiency of for-profit businesses and the incentives of market forces to bear on global social problems in a way that neither pure capitalism nor pure charity has been able to match.

Gregory Dees, one of the "fathers" of the field of social entrepreneurship (Dees 1998), says that *social entrepreneurs play the role of change agents in the social sector by:*

1. *Adopting a mission to create and sustain social value (not just private value)*
2. *Recognizing and relentlessly pursuing new opportunities to serve that mission*
3. *Engaging in the process of continuous innovation, adaptation, and learning*
4. *Acting boldly without being limited by resources currently in hand*
5. *Exhibiting a heightened sense of accountability to the constituencies served and for the outcomes created*

An entrepreneur and a social entrepreneur have the strong motivation to pursue their vision relentlessly and realize their ideas in common. However, what makes social entrepreneurship distinct from traditional business entrepreneurship is its **focus on the social/environmental mission**. This is true no matter what legal structure the social entrepreneur chooses.

For-profit social enterprises put mission before profits, typically using their excess revenues as a means of scaling the reach of their mission. **Nonprofits** are increasingly finding that they cannot rely on philanthropy to sustain themselves, much less grow. Thus, they are pursuing earned income strategies that leverage the organization's excess capacity and capability. By law, the earned income they generate must be reinvested in the enterprise and its mission. **Hybrid social enterprises**, which combine features of both for-profits and nonprofits, use this legal structure to expand potential revenue streams, all aimed at increasing and sustaining the organization's ability to pursue its mission (Lyons 2012).

Measuring the performance of a social enterprise is much more complex than it is for a commercial business, which can simply measure financial success. Measuring and monetizing lives saved, quality of life increased, and environmental damage mitigated (among other impacts), though possible, is exceedingly difficult to do. However, there are great examples that showcase the potential of this sector to benefit large numbers of people.

A Few Great Examples

WaterHealth International (http://www.waterhealth.com) is solving the problem of clean drinking water: 3.6 million people die each year from water-related disease. The social enterprise uses a franchising system, providing village entrepreneurs with UV filtration technology that allows processing and selling clean drinking water to remote villages at a low cost. Through its network of franchises, WaterHealth provides access to pure and safe drinking water to half a million people in four different countries.

There are many charitable water projects, but they have difficulties in pursuing their mission, as they do not have money for maintenance, for example, for fixing the pumps when they break down. On the other hand, WaterHealth, through the franchising system, has a network of entrepreneurs who pay for maintenance to troubleshoot equipment. Thus, the franchising system allows these initiatives to be sustainable. The model is not applied only by WaterHealth International, but also by other social enterprises that handle the problem of clean water delivery, such as 1001 fontaines (http://www.1001fontaines.com/en).

Another great example of social enterprise is the one of **Sulabh International** (http://www.sulabhinternational.org/), an India-based organization that works to promote human rights, environmental sanitation, nonconventional sources of energy, waste management, and social reforms through education. Sulabh International counts 50,000 volunteers and is the largest nonprofit organization in India.

Sulabh was founded by Bindeshwar Pathak in 1970, with the mission to rescue the **untouchables** (or scavengers, the poorest cast in India) from the subhuman occupation to remove raw (fresh and untreated) human excreta from buckets or other containers that are used as toilets or from the pits of pit latrines. Since 1993, the employment of manual scavengers was officially prohibited in India but is still taking place to this day.

Bindeshwar first developed a scavenging-free two-pit pour flush toilet (Sulabh Shauchalaya) as well as a safe and hygienic on-site human waste disposal technology that enabled the users to throw the excreta themselves in a clean way, without having to make use of the Untouchables. Sulabh created several solutions that were positioned to serve both the poor and the rich families, so that the high-end products could compensate the very low price proposed to the poorest families.

The social business was further developed through a new concept of pay and use public toilets, popularly known as Sulabh Complexes with bath, laundry, and urinal facilities being used by about 10 million people every day.

The innovation is an open-sourced technology that treats excreta and generates:

- Biogas, which is converted into electricity to power the building
- Biofertilizer, which is then sold at market price
- Treated water, which is used for agricultural use

The exceptional environmental impact of Sulabh is further complemented by the setup of English-medium public school in New Delhi and also a network of centers all over the country to train boys and girls from poor families, especially Untouchables, so that they can compete in the open job market – and finally become *touchables*.

Sulabh is one of the best examples of social enterprise that is economically sustainable. It maximizes environmental quality and social equity, using a business approach to solve a complex problem that governments and institutions have failed to address.

But the greatest innovation of all is that **Sulabh's toilet block blueprints are open source;** therefore, other organizations and people who are affected by the same problem can now use the solution and improve it. Innovation is no longer limited to the organization and its activities, but it can be further developed by other stakeholders, who can participate in the development process.

The Importance of Stakeholders Participation

There is another feature that distinguishes social entrepreneurship from business entrepreneurship: social entrepreneurs are held to a higher standard of accountability. Business entrepreneurs are accountable only to their customers and shareholders, whereas social entrepreneurs are accountable to a much larger group – **their stakeholders**, or "any group or individual who can affect or is affected by the achievement of the firm's objectives," according to Freeman's widely accepted definition (Freeman et al. 2010). This group includes part investors, as well as employees (including volunteers in nonprofits), direct beneficiaries, and the local community and the society.

Stakeholders have the chance to influence the decision-making process, providing opportunities to further align business practices with societal needs and expectations, helping to drive long-term sustainability. They also must be taken into

account by the organization when facing complex conditions in the operating environment.

Companies like Vodafone (Vodafone Corporate Social Responsibility Report 2014) engage their stakeholders in dialogue to find out what social and environmental issues matter most to them about their performance to improve decision-making and accountability. Such practices are key to mitigate risks, helping the practitioners to compete in an increasingly complex and ever-changing business environment, while at the same time, bringing about systemic change towards sustainable development (Jeffery 2009) (Fig. 1).

There are different stakeholder engagement approaches:

- **Pull communication** (*one-way engagement*: Information is made available, stakeholders choose whether to engage with it)
- **Consultation** (involved, but not responsible and not necessarily able to influence outside of consultation boundaries. *Limited two-way engagement*: organization asks questions, stakeholders answer.)
- **Partnerships** (shared accountability and responsibility. *Two-way engagement* joint learning, decision-making, and actions).

Through stakeholder engagement processes, organizations have positive economic results and creating win-win situations. Through the better understanding of the stakeholder needs and desires in consultation processes and through participation

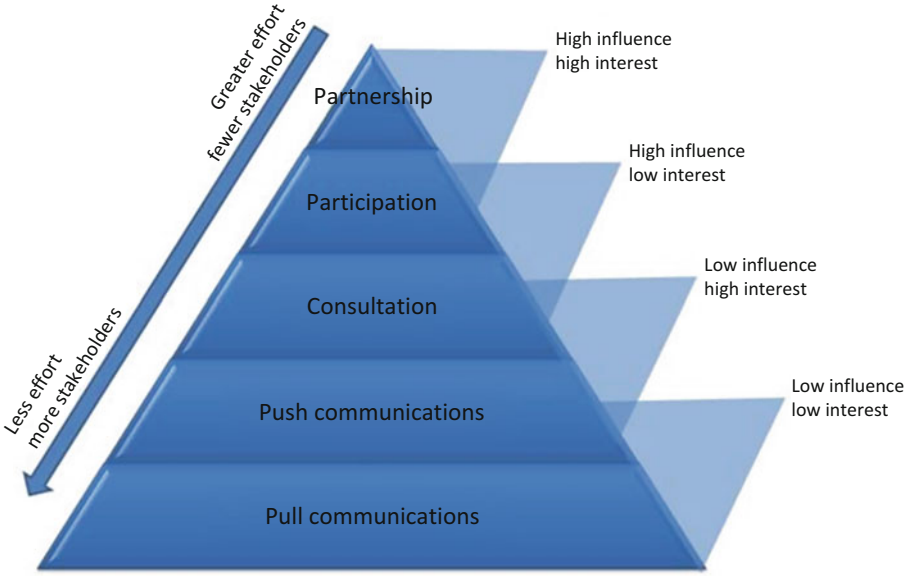


Fig. 1 The relationship between stakeholder influence/power and stakeholder engagement approaches (Stakeholdermap, 2015, Source: http://stakeholdermap.com/stakeholder-engagement.html)

and partnerships, organizations can identify and create win-win situations with those stakeholders. The underlying idea is that partnerships between businesses and other sectors can drive sustainable development.

Anticipating the potential in stakeholder dialogues at an early stage and following a step-by-step guide can lead to **successful shared value creation**. A great example of shared value creation is **Gram Vikas** (http://www.gramvikas.org), a social enterprise and rural development organization headquartered in Orissa, India, that assures access to basic education and adequate health services. The entire value creation process of Gram Vikas' involves "participatory decision-making, shared responsibility taking, and equal opportunities" with various stakeholders and particularly disadvantaged groups. The results are that each of these groups is assuming ownership of the solution and its delivery and thus the success rate is very high.

The trend towards cross-sector collaboration and stakeholder engagement is clear. The question is whether we are moving towards a convergence of values and whether shared value creation (expanding the total pool of social and economic value) will become the norm. Could the gap between social entrepreneurship and entrepreneurship be closed by actually making it so that every enterprise is responsible, transparent, and engages its stakeholders in the decision-making process?

The Age of Open Innovation

Individually, we are a drop, together, we are an ocean.

The twenty-first century is the era of mass innovation with more ideas, knowledge, and information being shared by more people than ever before.

Knowledge has become the key resource in the postindustrial society (Bell 1974); thus, reliance solely on internal innovation processes has become insufficient. Open innovation represents the logical result of dramatic social, technological, and environmental change, and it describes how organizations work with large groups to achieve greater results than any team of experts working alone.

For Henry Chesbrough, one of its pioneers, open innovation is "*the use of purposive inflows and outflows of knowledge to accelerate innovation. With knowledge now widely distributed, companies cannot rely entirely on their own research, but should acquire inventions or intellectual property from other companies when it advances the business model*" (Chesbrough 2006). The process has become increasingly essential, if not inevitable.

"Wisdom of the Crowd" processes have taken place in various forms and in many areas for decades. But it is now, in the information or digital age, that they are being exploited at such a fast pace.

Innovation challenges, hackathons, and external product development are all new phenomena that can best be summarized under the concept of open innovation.

The phenomenon that paved the road for a completely new approach to working together was the open-source culture. The term "open-source" refers to a software development strategy in which the source-code is made available to a community. This way, everyone can make changes and improvement to the software.

An example of the success of this strategy is the globally established computer operating system, Linux, which benefitted from the ongoing analysis, review, testing, and contributions of a large and diverse group of people from all over the world.

Wikipedia is another famous example of open source culture. It has over 80,000 contributors who have written more than 15 million articles in over 250 languages.

Traditional encyclopedias such as Microsoft Encarta or Britannica did not see the crowdsourcing phenomenon coming and continued to source their articles from few experts.

After some resistance, Microsoft decided to abandon its encyclopedia, acknowledging what everyone else realized long ago: it just could not compete with a free, collaborative project, where volunteer editors quickly update popular entries. Encarta simply could not keep up to the pace and was embarrassingly outdated.

> *The open source approach to collaboration enables people from all-over the planet to engage and create togther* (Rayner 2011)

Open innovation is also changing the way organizations work. A few corporations immediately realized the potential. LEGO, in its darkest days, tapped into abundant external talent to help them succeed in the face of some of their greater challenges. Back in 2003, the company was on the verge of bankruptcy. Under the lead of a new CEO, Jørgen Vig Knudstorp, the company successfully reached a passionate group of smart and enthusiastic people who were very familiar with their products and were just waiting to contribute: their customers.

They had hoped to get support from 100 of these fans, and they were inundated with responses from 10,000.

The community shared creative ideas and helped the company in prioritizing which ones were the best and had the greatest potential to become profitable. LEGO overcame its crisis and today, it still develops this process of creative collaboration, by involving passionate people outside of their internal structure.

We are shifting from a world in which everyone seems a competitor towards a world in which the upside of opening up and engaging with people and ideas from elsewhere outweighs the risk of sharing confidential information. Innovation can come from any source, and the organizations that are succeeding in inspiring external talent to engage in their crowd-storming process are gaining a strong competitive advantage compared to those who still uniquely rely on internal resources.

Companies like Apple and Google also depend on the effort of outside talent in the form of apps and open-source software.

After the launch of the iPhone in 2007, Apple switched the focus from the phone functionalities towards applications (or apps) that can be run on the iPhone to give it new capabilities. Apps demonstrated in a countless number of ways that the iPhone can become much more than a phone. For example, through apps you can read a restaurant customer review, find a cab, buy a book, split a restaurant bill, find a hotel, or translate speech into a foreign language. In 2012 alone, Apple paid $4 billion to apps developers and created 210,000 jobs related to the app economy in the United States.

In the same way, Google and Apple depend on open-source software that has been developed, used, tested, and improved on an open-cooperative environment. While Android derived from the Linux operating system, Apple used a package of open-source products called Darwin.

According to former P&G CEO (Lafley, 2008): "Innovation is a social process. And [it] can only happen when people do that simple, profound thing – connect to share problems, opportunities and learning. To put it another way, anyone can innovate, but practically no one can innovate alone."

The paradox of open innovation lies in the conflict between the potential benefits of collaboration and the prospects of knowledge leakage and misappropriation of the results of the process. The process is based on two-way interaction that may cause the organization to lose control of specific information. This knowledge, in the hands of a competitor, could compromise the competitive advantage potentially gained from the open innovation process. However, recent research focused on the significance of value creation through stakeholder engagement (Svendsen 1998) and offers a model that addresses this inherent conflict in open innovation processes.

Stakeholder participation removes the structural tension of open innovation (Gould 2012). Consideration of the social, organizational, and ethical benefits of engagement with relevant stakeholders enhances the concept of open innovation, helping to move beyond its solely practice-based origins.

The Love Story Between Open and Social Innovation

The concept of open innovation is very much associated with the business sector only; and in such a way, Chesbrough defines open innovation as a process taking place mainly in commercial research and development, reducing it to product development.

However, seeking ideas and solving problems is just one of the many facets of open innovation, and there are several reasons for expanding this paradigm shift to social innovation.

In fact, open innovation and stakeholder engagement towards collective social responsibility describe similar organizational processes: organizations reach outside their boundaries to access and share essential information with their stakeholders and with the crowd. Yet the two concepts, and their associated languages and discussions, have remained isolated from each other.

There is a vast potential to **co-create social value** through open and transparent networks that involve a diverse range of stakeholders, thanks to the ease of online collaboration tools and social media.

A few relevant initiatives started to emerge in the social sphere, creating a completely new field called **open social innovation**.

As previously mentioned, stakeholders' participation brings even more value when it goes beyond just listening to the people who can affect the organization,

and a process of co-creation is put in place. Modern information technology is a key enabler for empowering stakeholders and facilitates their participation in the development process: people can share their knowledge and exchange ideas; each one comes with incremental improvements and together can benefit from the collective wisdom of a crowd.

A fantastic example of the power of open-social innovation is the R&D-I-Y, *research and develops it yourself*: a process that has been applied to the Windowfarms network (Pearl 2011).

Britta Riley is the cofounder of Windowfarms.org, a New York-based company that makes hydroponic platforms for growing food in city windows, designed with the help of more than 1800 enthusiastic collaborators from all over the world.

Britta took her inspiration from NASA, which uses hydroponics to explore how to grow food in space. She reasoned that many apartment windows have less than stellar conditions for growing plants, especially in a Northern winter. Conditions in any particular window would limit what could grow there – but perhaps hydroponics could contribute to food security on earth.

Britta decided to open source the project. She published the design on the web and invited anyone from anywhere in the world to improve the system. With no intellectual property issues, it was open to co-developers. Collaboratively, they have developed a system that grows a salad a week in an apartment window and allows an individual to cut their carbon footprint nearly in half.

On a global scale, the project has taken on a life of its own. Enthusiasts in Finland are working to customize the system with LED grow lights, also developed collaboratively, so that they can continue their gardens during the long, dark winter. Other contributions include air pumps to replace water pumps and optimum nutrients for strawberries that result in fruit throughout a New York winter. Britta says that the real reward from working with this company is the joy of collaboration.

Many other examples of stakeholder's participation through open-innovation deserve the right attention.

People co-create concepts through open content systems such as Wikis – these web applications have led to fascinating examples of collective intelligence. Wikipedia has inspired many organizations to create their own versions or copycats. This is the case of Energypedia, a project of German development agency, GIZ, that combines local and global knowledge to collect experiences and best practices in water and sanitation issues.

In the wake of the Fukushima nuclear disaster, Japanese citizens set up a network of volunteers, publishing radiation levels they measured themselves after that trust in official data had collapsed.

Volunteers and political activists also take advantage of the Internet and tech devices such as mobile phones, tablets, etc., to monitor events and issues taking place around the world. Ipaidabribe.com, an anticorruption project, allows ordinary citizens to send messages denouncing cases of corruption.

However, the best example of open-social innovation is the one of Foldit, an effective online tool that combines advanced gamification techniques with crowd collaboration to contribute to cancer and HIV/AIDS research.

The Fold it Example

Foldit is an online puzzle video game about protein folding that was developed by Adrian Treuille. It is part of an experimental research project developed with the University of Washington's Center for Game Science in collaboration with the UW Department of Biochemistry.

The public beta version was released in May 2008 and has 240,000 registered players. The objective of Foldit is to fold the structures of selected proteins as well as possible, which is one of the hardest and most expensive problems in biology today.

The protein biosynthesis is reasonably well understood, as is the means by which proteins are encoded as DNA. Determining how the primary structure of a protein turns into a functioning three-dimensional structure and how the molecule "folds" is more difficult; the general process is known, but predicting protein structures is computationally demanding.

Foldit is an attempt to apply the human brain's natural three-dimensional pattern matching abilities to this problem. By analyzing the ways in which humans intuitively approach these puzzles in the game, researchers improve the algorithms employed by existing protein-folding software. As more players complete more puzzles, the researchers can create a better understanding of these protein structures and craft new medicines to promote better health and cure disease.

Although at the beginning, gamers were playing on folding proteins to which the solution was already known, now Foldit is being used for real-world scientific problems.

A report by an international team of researchers from the USA, Poland, and Czech Republic in Nature Structural and Molecular Biology unraveled that Foldit players have solved the crystal structure of Mason-Pfizer monkey virus (M-PMV) retroviral protease (Khatib et al. 2011).

Retroviral proteases have critical roles in viral maturation and proliferation, and they are very important for antiretroviral drug development for diseases such as AIDS. For over a decade, researchers have been unable to solve the structure despite using many different methods. Even recently, the protein-folding distributed computer program, Rosetta, which uses thousands of home computers' idle time to compute protein structures, was not able to give an answer. The Foldit players, using human intuition and three-dimensional pattern-matching skills, however, were able to solve the problem within days.

Collective Social Entrepreneurship

Social entrepreneurship has been considerably growing in the past 30 years, but it still remains a small part, only 6.5% of the entire economy in Europe (Seforis Consortium 2013).

On the other hand, the explosion of global challenges in areas such as climate change and environmental degradation; inequality and poverty; lack of access to

basic healthcare, clean water and energy; mass-migration and international terrorism requires modern sustainable enterprises to apply a more radical involvement of all their stakeholders.

Thus, to achieve true impact, social enterprises need to find a way to go beyond making progress on their own; they need to lead collaborations with others (Milway 2014). Creating a sustainable ecosystem would require individual social enterprises to collaborate not just within their sector but also across sectors. Montgomery et al. (2012) term such collaboration "**collective social entrepreneurship.**"

According to Robert Wayne Gould (2012), this can be realized through a combination of open innovation and stakeholder participation.

In the previous paragraphs, we have seen how collective intelligence can be extremely effective at tackling complex problems. On the other hand, we have analyzed the importance of stakeholders' engagement to support social entrepreneurial organizations to produce long-lasting impact for the common good.

Thus, to initiate a new societal paradigm based on open-source collaboration, all stakeholders need to be empowered to voice their concerns and participate more actively in the decision-making process.

The participation, investment, and inclusion of all members of society in the development process is the key to not only help people fulfill their human potential, but also to ensure that full advantage is taken from a country's human resources, as well as to promote peace and stability.

One of the main organizations democratizing the participation of stakeholders in the development process is IDEO.

About OpenIDEO

OpenIDEO is an open innovation platform on which global communities can take part in solving any of the various challenges presented on the platform. It is an online international community enabling people to collaborate in developing innovative solutions to pressing social and environmental challenges. Everyone can participate: veteran designers, critics, academics, and the curious lurker.

Similar to a formal innovation process, ideas are presented as "challenges." One such challenge was initiated by Jamie Oliver to raise children's awareness of the benefits of fresh food so they can make better choices. Challenges make progress through various creative phases: inspiration, concepting, evaluation, refinement, and implementation.

The first step is called **inspiration**. The process starts with research to develop empathy and understanding on the topic: capturing people's needs and experiences before diving into solutions. Contributors are encouraged to submit inspirations in the form of images, stories, and visuals. During the next phase of the project, **concepting**, contributors are asked to post a solution. People are invited to comment and ideas owners are encouraged to incorporate the feedback received and then refine their ideas again. This iterative approach is based on the philosophy of learning through building – trying out ideas with real people as quickly as possible.

Next, members are asked to rate and comment on concepts in the **evaluation** phase because each concept will gain merit depending on the community response. Only the best concepts carry forward.

In the next step of the design thinking process, called **refinement**, IDEO facilitators tweak the evaluated ideas, adding a highly focused design approach to it. This phase is to be understood through Tim Brown, writing on his blog, "*The idea of crowdsourcing innovation is, in my view, still a big experiment. Conventionally, the question has been whether the crowd can outperform the internal team. Our view is that small teams are good for some things and the broader community is good for others. The goal of OpenIDEO is to find out whether it is possible to orchestrate collaboration between the two to achieve better results*" (Brown 2010). The results of OpenIDEO are impressive. Within 5 years, they managed to post 29 challenges and over 80,000 people participated, submitting over 6000 ideas. Out of them, 300 projects are in the development stage.

Open Lean Innovation

Another interesting trend that is converging with the crowdsourcing universe is the Lean startup methodology, which was coined by Eric Ries from his study of Lean Manufacturing techniques created by Taiichi Ohno and Shigeo Shingo of Toyota.

The lean thinking became particularly relevant after the Dot-Com bubble of the late 1990s, in which companies like Pets.com and Webvan could raise huge amounts of capital, spending it as fast as they could raise it, only to collapse when common sense re-asserted itself and the bubble burst.

After the bubble, venture investors spent the next 3 years doing triage, sorting through the rubble to find companies that were not bleeding cash and could actually be turned into real businesses. Startups began to recognize that they were not merely a smaller version of a large company. Rather, they understood that a startup is a temporary organization designed to search for a repeatable and scalable business model. This meant that startups needed their own tools, techniques, and methodologies distinct from those used in large companies.

The "lean startup" favors experimentation, overelaborate planning, customer feedback over intuition, and iterative design over traditional "big design up front" development. Although the methodology is just a few years old, its concepts, such as "minimum viable product" and "pivoting," have quickly taken root in the startup world, and business schools have already begun adapting their curricula to teach them.

The unit of progress for Lean Startups is **validated learning**, a rigorous method for demonstrating progress when one is embedded in the soil of extreme uncertainty. Validation comes in the form of data that demonstrate that the key risks in the business have been addressed by the current product. The lean startup asks people to figure out the right thing to build and the thing customers want and will pay for, as quickly as possible.

Modern entrepreneurs need feedback on their solution. They want to know when it is going to fail. They have to know who will use it, and who won't. They need to know how much they are willing to "pay" for it. That information won't be found "pitching" a solution.

Thus, the startups that ultimately succeed go quickly from failure to failure, all the while adapting, iterating on, and improving their initial ideas as they **continually learn from customers**.

Each stage of a startup development is highly iterative. Customer feedback is essential to learn everything: from the problem that the product should solve, to the best communication or distribution channel, as well as the revenue model and the pricing. This continuous collaboration with the customers is key to reduce the inner uncertainty within the innovation process.

As in the case of open innovation, there is a paradox between the benefit of opening a project to the feedback of the customers, and the fear that several entrepreneurs have that their idea will be stolen. Thus, they often prefer to develop their project in secrecy.

However, several economists and successful entrepreneurs support the concept of sharing business ideas. For example, Nilofer Merchant (2012), in her article, "Let your ideas go" in the *Harvard Business Review*, or Patrick Hull (2013) in *Forbes Magazine*, "Talk about your idea, it won't get stolen." They strongly believe that ideas cannot be stolen, because the hardest task in creating a startup is not having the idea, but implementing it. Timing and execution are the essential elements to succeed.

If we apply the concept of lean startup to social innovation initiatives, then it becomes fundamental for social entrepreneurs to involve their stakeholders in the process of validating the organization strategy, promoting full transparency from the financial performance to the resulting social impact. At the end of the day, young social enterprises face the same challenges of traditional startups: they often lack the resources to succeed (knowledge, network, and skills) and they operate in conditions of extreme uncertainty, which, according to *Forbes*, causes 8 out of 10 startups to fail in the first 2 years of activity. Thus, by opening up and enabling the mentors, peer entrepreneurs, and stakeholders to contribute with their knowledge in the business modeling process of social businesses, we can considerably increase the chances of success of these organizations and scale their impact (Potter 2014).

Furthermore, this open approach to social innovation will be the key to enable NGOs to shift their revenue model (based on traditional philanthropic donations) towards the one of sustainable social enterprises. A recent OECD report showcases the decline in official development assistance, reinforcing the need for NGOs to decrease their dependence from external financial support. The opportunity for social projects to crowd-source consulting from their stakeholders to evolve their strategy is probably the greatest hope that we have to revitalize the third sector.

A great example of stakeholders' participation to validate the strategy of social entrepreneurs through crowdsourcing is the open innovation platform, Babele.

BABELE: Crowdsourcing Business Models for Social Entrepreneurs

Babele (www.babele.co) is a social enterprise launched in the fall of 2013, with the objective to harness collective intelligence to help social enterprises and CSR-driven projects to validate their key assumptions and co-develop a sustainable strategy through stakeholders' engagement and participation. The ecosystem hosts a community of over 800 CSR projects and social businesses from 103 countries (www.babele.co/#!/projects).

BABELE is derived from the idea that combining collective human brain power and modern information technology has the potential to form just such an innovative channel for the generation of sustainable development projects.

The platform has a unique open-source approach for supporting social entrepreneurship and creating social impact. It has been inspired by the emerging paradigm of more open, collaborative, and adaptive organizations. Instead of creating social business strategies in secrecy and thus reinventing the wheel without learning from others, it offers an advanced system to share ideas, get inspiration from others, and co-create business strategies for social good and replicate them in other parts of the world.

As Dom Potter explains in Stanford Social Innovation Review: "*Open structures allow for social construction of products and services. This is where the real potential of approaches such as design thinking and lean startup are rendered into concrete actions; they push us to develop products and services with and not for our market.*"

The platform combines the principles of **social entrepreneurship**, **crowdsourcing,** and **lean startup,** engaging crowds of stakeholders in problem-solving, supporting the business development process of social enterprises from all over the world.

Instead of a small number of people setting up definitions of what it means to be a social organization and acting as regulators without a societal mandate, the platform enables to move toward a distributed model of regulation – a model where each and every one of us has the opportunity to look into the workings of any organization and make his/her own judgment.

About the Platform Features

The platform provides a business modeling framework that enables entrepreneurs to develop their ideas into a structured blue print. The project team can co-create the strategy, aligning every member on the fundamental underlying assumptions of the business model.

The collaborative part, in which people can debate, share ideas and give feedback, comes with the stakeholders engagement.

The team can invite mentors and supporters and organize them in groups. Every group will be given different privacy access to the strategy, the files, and the discussions related to the project.

The idea is that every different stakeholder group has a different impact on the project strategy and key activities. For example:

- *Beneficiaries* are key to assess the project's outcomes and social impact.
- *Customers* can help validate and improve the product or service value proposition.
- *Suppliers and distributors'* input is key to improve activities and processes.
- *Partners'* involvement can lead the organization to achieve as many win-win collaborations as possible.
- *Advisory board* can help with strategic decisions regarding the company performance.
- *Investors* are key to support the organization's growth.
- *Supporters/Facebook likers* are also a very useful resource that can help through problem solving and decision making.

Therefore, Babele transform innovation into a highly collaborative process. It enables stakeholders to participate and collaborate to the on-going co-development of sustainable projects and impact ventures. It exposes entrepreneurs to valuable feedback and validation since the conception stage, thus increasing the chances to render its vision and potential into reality.

In addition to this, the platform enables the entrepreneur to organize all the shared content through a tag system, and most importantly, it enables to tag the skills and competences that are required in every discussion/challenge. One of the major issues with today's interconnected society is the high chance to be overloaded with irrelevant information.

Therefore, filtering people according to their field of expertise allows the entrepreneur to maximize the chances to receive relevant feedback, while preventing mentors to receive invites to discussions that might not be of interest.

Open Business Modeling at the Ecosystem Level

Babele provides public and private mentoring communities for organizations supporting social entrepreneurship, such as University classes, mentoring programs, incubators, accelerators, MOOCs, corporate CSR programs. Babele helps them to leverage the collective wisdom of their networks: academics, business experts, coaches, partners, collaborators, entrepreneurs, and employees can bring an unprecedented amount of knowledge to help social ventures refine their business model, considerably increasing the chances of success of these organizations.

- **Entrepreneurs** are invited to refine their business model, validate their assumptions, and tackle key growth challenges by capitalizing on the ideas and feedback of the mentors in the community.
- **Mentors** are matched to the ventures according to their interests and competences; they can track the work done by each team and contribute by submitting ideas, sharing documents and giving feedback to each section of their strategy.

- **Program Administrators** can manage people and ventures, can customize the business framework according to the program best practices, and can assign roles, share insightful files, videos and articles, and catalyze conversations around those shared insights.

These online communities work as a support tool to the off-line components of the programs. In fact, the online format is not meant to replace the offline interaction. The trust between mentors and mentees, as well as the community engagement, is better created off-line.

On the other hand, sharing of best practices, peer learning, and knowledge transfer are better managed online, mostly when the group goes beyond the 40 people. Therefore, the Babele team works closely with the administrators to find the right balance between the online and offline activities for each program, while taking into account the program key goals and the key network constraints.

Towards The Network of Networks

Despite a dense ecosystem of organization propelling social innovation is emerging, many of these actors are often not effective in developing and accelerating social enterprises. Aside from a few elephants in the room (such as Ashoka, Acumen plus, Skoll foundation) that have funding and visibility, the rest of the market is highly fragmented.

There are a myriad of small incubator, accelerators, classes, startup weekends, etc., that are managed by small teams, with very scarce resources, that are doing their best to support social entrepreneurs.

Despite their effort, the failing rate of social enterprise is still too high. Most social entrepreneurs often lack the necessary business acumen to build a viable business model, prioritize their actions, and find partners.

Statistics reveal that 8 out of 10 newly created initiatives fail in realizing their objectives.

Most of these small support programs are struggling to cooperate with other actors in the ecosystem. Rarely, they succeed to involve pro-bono corporate and institutional mentors on-board that could bring priceless know-how and network connections to help the entrepreneurs succeed. Many programs are struggling to provide a good follow-up support to alumni or provide the initial 5000€ most start-ups need to simply validate that there is a market for whatever solution they want to create.

According to GALI's report "What's Working in Startup Acceleration," the 4 high-performing programs from the study had an average spend of $140,321, which is more than $60,000 more than the average for the four low-performing programs.

In reality, these sums are way beyond the budget of the majority of the programs out there.

The high market fragmentation is bringing many support programs to fail. According to Tech Crunch: "While a few top-tier programs get the cream of the crop unicorns of the future, the hundreds of others struggle to attract teams that will produce the investment-grade companies on which their models so depend."

Ultimately, the **market disconnection** is responsible for the lack of development in the mechanisms and institutions that channel information and money between funders and social ventures.

Babele is tackling this problem by embracing the philosophy of creating the **network of networks for social innovation.**

An open paradigm can enable all these small programs supporting social-change to learn from each other, share experts, track the progress and performance of entrepreneurs, and funnel alumni towards the programs that could help them with their next steps in the journey to build a sustainable and mission-driven company.

Babele is actively working to connect the dots between these networks and organizations, offering opportunities for collaboration and cross-pollination. The final result is a network of communities that can interact with each other: social innovation actors, entrepreneurs, incubators, universities, municipalities, citizens, or CSR-driven companies.

This approach is fundamental to consolidate the social innovation market, incentivize openness and transparency, and support the replication of the best initiatives that have the potential to address the most urgent challenges of our time (Fig. 2).

Ultimately, Babele aims to tap on the collective knowledge of society stakeholders to solve local and global issues, facilitating peer-to-peer learning and sharing of best practices, while removing geographic boundaries between the different organizations and initiatives.

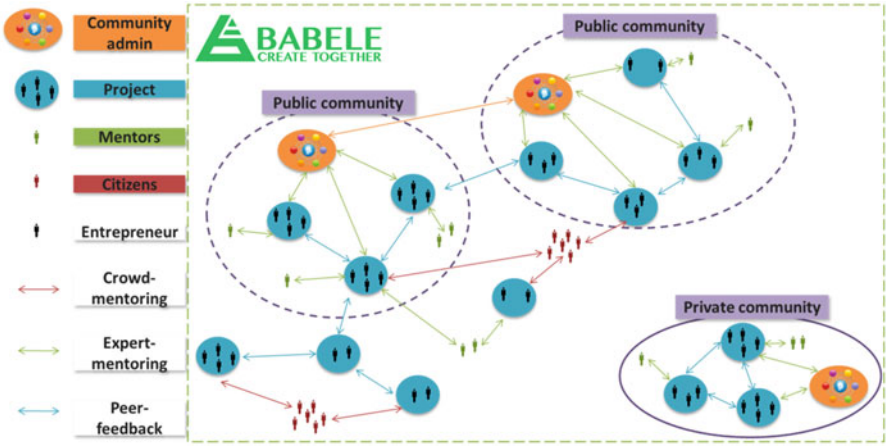


Fig. 2 Interactions within the Babele platform between independent projects, projects within public and private communities, mentors, citizens, and peer-entrepreneurs (Babele, 2015)

Beyond R&D Through the Power of Networks

Robert Fabricant (2013) discusses if social enterprises can be seen as R&D labs in an insightful article titled, "Meet Your New R&D Team: Social Entrepreneurs" in the *Harvard Business Review*. According to him, social entrepreneurs can have a "R&D function" for learning how to serve underdeveloped markets; they are innovative and find solutions to dedicated social issues. Once their solution has a proven impact, they should scale-up. To do this, they need more resources. Therefore, partnering with corporate CSR initiatives may offer them the necessary means to grow. There are many examples; Robert Fabricant describes four of these partnerships in his article.

This point of view is not new. What Robert Fabricant mentions are, in fact, "hybrid strategies," which means creating partnerships between social entrepreneurs and multinational companies. Oliver Kayser, after 18 years with McKinsey and 5 years with Ashoka, has created Hystra consulting, a company specialized in these hybrid strategies. "*Across the world, social entrepreneurs have been experimenting with a mix of social and business strategies, gaining new insights into market needs, and coming up with innovative solutions to intractable global problems. It is now time for concerned and conscientious corporate leaders to do what they do best in order to help social solutions achieve the scale needed to change the world,*" he says (Kayser 2009).

Both Robert and Oliver recognize that social entrepreneurs bring innovative solutions to social issues and therefore are doing "R&D." However, they also acknowledge that social enterprises need to partner with multinational companies to grow their scale and scope.

If we continue with the metaphor where social enterprises are the "R&D Lab" for Europe social challenges, then corporations are the "production" department that deploys the prototype conceived upstream.

Their point of view remains in the current paradigm, where only the corporations have the force to scale-up from the prototype model to consistent production. They are the only ones capable of doing this because social enterprises are too small and do not have enough resources.

Now imagine a new paradigm where social enterprises would not only be the "R&D lab" but also the "production" department. They would be interconnected within an efficient network, where they collaborate, experiment, and exchange in a transparent way.

This statement might sound absurd, but it will become less hard to believe through the following comparison. In the 1980s, we had super-computers ("corporations") that were extremely powerful in comparison with any standard computer in the market ("social enterprise"). Now with the power of the Internet ("our efficient network"), many interconnected PCs have become more powerful than a supercomputer.

A new ecosystem can be created to gather the competencies and resources to make it happen where social enterprises will not only be the "R&D lab" of Europe's social issues, but they will be the engine solving these social issues and promoting a new kind of growth.

Open Governance

Open social innovation is contaminating several other sectors beyond social entrepreneurship.

Civic engagement is another key trend that combines the collective wisdom of the crowd (citizens) with the collaborative creation of sustainable initiatives that have the potential to improve the quality of life of local communities.

Governments are increasingly realizing that they can, and need to, communicate with citizens in a different way. Citizens can help provide better solutions for cities, but for that, they need to be included in decision-making processes. For example, in the German city of Nuremberg, citizens were asked to locate the noisiest areas of their neighborhood. By jointly identifying these spots, the city administration did not only get a different picture of the problems but could also work on much better solutions.

Multistakeholder governance appears to be the future way of developing public policy, bringing together governments, the private sector, and civil society in partnership. The movement towards this new governance paradigm has been most marked in areas involving global networks of stakeholders where it is too intricate to be represented by governments alone. Nowhere is this better illustrated than on the Internet, where it is an inherent characteristic of the network that laws, and the conduct to which those laws are directed, will cross national borders. This momentum has developed to bring multistakeholder governance to the Internet.

The United Nations e-Government Survey 2008 indicates that governments are moving forward in e-government; the UN e-participation index indicated a constant upward movement with 189 countries online in 2008.

More than 200 municipalities and public institutions are estimated to have initiated participatory budgeting in the world.

Meu Rio

A magnificent example of this phenomenon is the online platform, MEU RIO, which allows the citizens of Rio de Janeiro to have a say in what is happening in the city.

Alessandra Orofino, founder of the initiative, explains in an interview that their main work is the one to translate public policy issues into a language that is understandable to broader society and young people. The site gives people an opportunity to act on things they think are important and allows both organizers and users to identify areas for change and action. Meu Rio has a team dedicated to researching public policy so they can mobilize people effectively.

As an example, in 2013, an 8-year-old student wrote to Meu Rio about her school, the Escola Municipal Friedenreich. It has around 300 students and is one of the best public schools in the country along with specialized staff and facilities for the disabled.

The city had decided to demolish a school to build a parking lot for the nearby Maracanã Stadium. There was no plan to rebuild the school or transfer the students,

and the parents only found out through the local news. So the organization set up a campaign to save the school and got 20,000 signatures on a petition. The campaign started attracting media attention, but even the secretary of education did not know what to do. So Meu Rio decided to try a new tactic. They set up a webcam at an apartment across the street from the school and monitored the school 24/7 through a website with a live feed from the camera. People could sign up to be a "guardian" of the school and watch the feed, and if bulldozers showed up, those watching could press a red button to contact Meu Rio, which would send out text messages to followers to physically protect the school. Around 3000 people signed up to watch the school, using analytics, Meu Rio discovered that for the 2 months of the campaign, not a minute passed that someone was not watching the school. Public officials realized it would be a PR disaster to demolish the school and gave up.

Towards Pure Participatory Democracy

People participation can go beyond idea brainstorming and problem-solving. The next step of stakeholders' engagement is the co-ownership of the common good solutions collaboratively conceived and implemented in the local communities.

A very small village in the middle of Lapland (Sweden) is living on the next edge of sustainable development and crowdsourcing, practicing as no one else co-creation for the common good.

The majority of Vuollerim's inhabitants have understood that while in a period of abundance, competition might be the best strategy, and in a period of scarcity, collaboration is certainly the approach that offers the best possible outcome.

Being in such a peripheral part of the world can present several challenges, such as the migration of young minds towards the bigger and more attractive cities in southern Sweden.

To address these challenges, the people of Vuollerim have come together and worked on a new welfare system that involves citizens in first person and embraces entrepreneurship as well as taking initiative. This initiative is based on collaborating for the common good rather than focusing on individual benefits.

The district of Vuollerim has about 800 inhabitants, 60 companies, and 40 nonprofit associations. All of these businesses and organizations have jointly agreed (by writing it in their statutes) to aim for local development and the best for the village.

It all started in 1999 when the first village-owned company was born to save the hardware store that had closed down and was about to be demolished. The Vuollerim's economic association is composed by more than 100 members who recognized how essential the hardware store was for Vuollerim and its surroundings. Together, they bought the property, which is now running as a multifunction store called "The Greenhouse," in the middle of the village.

Another great example is VIVA, which manages the Inn, a year-round open hotel. VIVA is co-owned by 150 citizens who have built and decorated the hotel in collaboration with several other villagers.

This democratic collaboration among citizens has also been extended to the educational field.

Vuollerims Charter School, "a good small school," is a village-owned company that was founded in 2009 and has over 100 co-owners. The reason to start a charter school in the district of Vuollerim was to ensure there was a complete primary school education available in the village, now and in the future. This had become a concern after the municipality's decision to close down the elementary school in Vuollerim for ages 6–9.

Another incredible collectively owned company is The Village Team, which provides innovators in all ages with the skills, experience, and expertise necessary to take their idea off the ground and develop unique, locally anchored, sustainable enterprises. These days, The Village Team business is in the start of implementing a crowdsourcing experiment in the open innovation platform, Babele, a tool for crowdsourcing ideas and co-developing smarter solutions in a collaborative way.

The Village Team contributes as a "mentor" and sounding board for the development of new business ideas. They choose the projects depending on the individual competences and interests of the members, as well as on the local needs anticipated for the village. Currently, the company engages in producing local music, renting out conference halls and vehicle storage, as well as offering copying and tire services.

Another village company is Lapland Vuollerim Welcomes You AB. It is a community-based tourism company, providing genuine "everyday life" experiences. Lapland Vuollerim has been nominated for Best Outdoor Product of the Year, World Responsible Tourism Award, and Tourism for Tomorrow Innovation Award, and it is a socially responsible business owned by villagers, reinvesting 100% of their profits into further growth of the company and into the local economy.

What is absolutely fascinating of this model is that all the above-mentioned companies strive to enhance both economic and social well-being and growth for the district. All profits for each village-owned company are reinvested in the district in one way or another.

This collaborative welfare model enabled Vuollerim citizens to work together towards a common goal: be better off as a community rather than having a village with winners and losers.

The village is on its way to a brighter future by retaining jobs, youth, and investing in education. This model is a true *hope* for all the peripheral areas in the world that are suffering from similar challenges. It can be done everywhere! The secret is to work together.

How Crowdsourcing and Social Innovation Can Favor Participatory Democracy

Crowdsourcing and design thinking can be smartly combined to funnel the participation of societal stakeholders, who can take an active role in the development of civic projects for the common good. The ideal open innovation platform to achieve participative local democracy should incorporate

elements of **design thinking**, as a way to funnel the creativity of the crowd toward the development of the most effective and feasible solution, and a **sustainable planning framework**, to use collective intelligence to define all the key elements of the project (from financial variables until its expected impact).

Below are the key phases that the ideal participatory democracy platform should contain:

Phase One: RESEARCH PHASE
In this stage, stakeholders work together to create a clear picture of the status quo:

- Identify the key local problems that negatively affect the livelihood of the municipality and gather all the relevant data (quantitative and qualitative) to describe the problem and how it occurs
- Collectively assess the root cause of the problems and analyze the resulting negative impact through an 8-dimentional framework, of which key variables are Political, Economic, Social, Technological, Environmental, Demographical, Cultural, and Legal
- Gather success stories, solutions, and best practices coming from other municipalities and contexts

Phase Two: IDEATION PHASE
In this stage, stakeholders co-propose the solutions with the potential to address the problem.

The ideation framework has to be basic to enable creativity in the crowd-storming process.

This will be composed by a short description of the solution, a presentation of why and how the solution has the potential to address the problem, necessary resources, and implementation complexity.

Phase Three: FEEDBACK AND SCREENING PHASE
In this stage, stakeholders dig deeper into the ideas with insights that will encourage idea development.

Stakeholders will also be able to vote their favorite ideas while justifying their choice.

By the end of this phase, the 10 most voted ideas will proceed to the following phase.

Phase Four: PLANNING PHASE
In this stage, the selected projects will be developed extensively through a collaborative project planning methodology.

Stakeholders will develop each idea into a complete implementation plan, which will include key activities, needed resources, key partners involved in the implementation, realization timeline, as well as a complete section with financials budgeting and expected social/environmental impact.

Phase Five: REFINEMENT PHASE
In this stage, stakeholders will examine each idea and give feedback to each aspect to further refine the proposed plans.

- Mentors and advisors are allocated to each project topic based on their key interests and competences.
- Project proposers can incentivize proactivity and collaboration by rating the work done by their peers.
- The companies, organizations, and institutions that could be involved in the implementation will help validate timeline and budgets for the realization of the projects.
- The municipalities will participate by sharing valuable data to assess each project feasibility.
- By the end of the phase, the community votes the best projects that will be implemented.

Phase Six: IMPLEMENTATION PHASE
In this stage, the winning ideas are announced and an agreement is established among the organization that will participate in the project implementation.

- A transparent and easy-to-digest reporting will display the project progress and performance against established Key Performance Indicators.
- A blog with problems and challenges will be shared with the community to benefit from the collective intelligence process also in this final stage.

If it is true that democracy is a process that must constantly be reinforced at all stages by the internal participation and action by the institutions of the state as well as the international community, then it is fundamental to create new platforms to enhance the discussion among principal societal stakeholders to spread awareness of the things that are known, discuss a strategy, and get societies together to solve the global issues. Through this process, the crowd can engage and create meaningful solutions for the common good of the municipality, bringing a new, fresh perspective to the current model of democracy.

Conclusion

The paradox of a global economy increasingly unified and a global society increasingly divided is the most dangerous threat that weighs on the planet, because it makes difficult if not impossible, the cooperation necessary to solve the other problems.

While market forces demonstrated to be a nonsufficient mean to lead to the most efficient allocation of resources, governments and institutions have failed to meet the needs of the Common Good and bring society together to solve global issues.

In addition to this, the concept of *homo economicus* is losing traction. People are not the rationally self-interested actor lurking at the core of mainstream economic theory (the homo economicus: a mercenary ready to crush their neighbors in order to maximize its own interest).

The critical unsustainable situation has led more and more people to realize that we need to create a new type of system. We can become **homo reciprocans**, if society promotes a development model based on sustainability, then people will act accordingly (Berlingen et al. 2015). We can see these values reflected in the new organizational models that pioneers are creating through social entrepreneurship and impact enterprises, Sulabh, Windowfarms, FoldIt are just some examples.

As a reaction of the public institutions failures to answer to the global need of common good, citizens are getting "smarter," more capable of interpreting issues and discerning between options on their own than simply accepting the views of media and political elites.

People started to realize that if we want to solve the biggest challenges of our time, it is not enough to delegate to someone else. We need a bottom-up, collaborative, and open-sourced approach, where people can actively participate in the development, implementation, and replication of social good projects.

Cyber-Democracy comes into play as the most effective approach to convert this new wave of crowd-participation into an organized platform to develop and replicate ideas, as well as encourage transparency and collaboration at a global scale.

The transparency created by Cyber-Democracy would act as a new ecosystem for differentiating and customizing socially responsible products and services, attracting stakeholders that could create added value previously unobtainable in the conception stage.

We believe such ecosystem has the potential to accelerate the paradigm shift towards a more sustainable market place.

References

Anderson, S., & Cavanagh, J. (2005). *Field guide to the global economy* (2nd ed.). New York: New Press. World Development Report, Washington, DC, World Bank (for country GDP data).

Bakan, J. (2004). *The corporation: The pathological pursuit of profit and power*. New York: Free Press.

Bell, D. (1974). *The coming of post-industrial society.* New York: Harper Colophon Books.
Berlingen, F., Gauthey, M. A., De Grave, A., Filippova, D., Guedira, A., Léonard, A., Mootoosamy, E., & et Maëva Tordo, B. T. (2015). *Société collaborative, la fin des hiérarchies*. Paris: Rue de l'Echiquier.
Brown, T. (2010). Blog post. Retrieved from http://designthinking.ideo.com/?p=482
Chesbrough, H. W. (2006). *Open innovation: The new imperative for creating and profiting from technology*. Boston: Harvard Business Press.
Dees, G. (1998). *The meaning of social entrepreneurship*. Kansas City: Kauffman Foundation and Stanford University.
Duhigg, C., & Baraboza, D. (2012, January 5). In China, human costs are built into an iPad. *The New York Times*. Retrieved from http://www.nytimes.com
Emerson, J., & Twersky, F. (1996). *New social entrepreneurs. The success, challenges, and Lessons of Non-Profit Enterprise Creation*. San Francisco: Roberts Foundation.
Fabricant, R. (2013). Meet your new R&D team: Social entrepreneurs. *Harvard Business Review.* Retrieved from https://hbr.org/2013/03/meet-your-new-rd-team-social-e
Freeman, R. E., Harrison, J. S., Wicks, A., Parmar, B. L., & De Colle, S. (2010). *Stakeholder theory – The state of the art*. Cambridge: Cambridge University Press.
Gould, R. W. (2012). Open innovation and stakeholder involvement. *Journal of Technology Management & Innovation, 7*(3).
Hull, P. (2013). Talk about your idea, it won't get stolen. *Forbes Magazine.*
Jeffery, N. (2009). *Stakeholder engagement: A road map to meaningful engagement.* Doughty Centre, Cranfield School of Management. Retrieved from http://dspace.lib.cranfield.ac.uk/handle/1826/3801
Kayser, O. (2009). In Ashoka to partner with Hystra to increase corporate engagement in scaling up social innovations. Retrieved from https://www.ashoka.org/press/5809
Khatib, F., DiMaio, F., Cooper, S., & Kazmierczyk, M. (2011). Crystal structure of a monomeric retroviral protease solved by protein folding game players. *Nature Structural & Molecular Biology, 18*, 1175–1177.
Korten, D. (2001). *When corporations rule the world* (pp. 60–68). Oakland: Kumarian Press/ Berrett-Koehler Publishers.
Leonard, A. (2007a). The story of stuff. Retrieved from http://storyofstuff.org/wp-content/uploads/movies/scripts/Story%20of%20Stuff.pdf
Leonard, A. (2007b). The story of change. Retrieved from http://storyofstuff.org/wp-content/uploads/movies/scripts/SoChange_Annotated_Script.pdf
Lyons, T. S. (2012). *Understanding social entrepreneurship: The relentless pursuit of mission in an ever changing world*. New York: Routledge.
Merchant, N. (2012). Let your ideas go. *Harvard Business Review.* Retrieved from https://hbr.org/2012/06/let-your-ideas-go
Milway, K. (2014). How social entrepreneurs can have the most impact. *Harvard Business Review.* Retrieved from https://hbr.org/2014/05/how-social-entrepreneurs-can-have-the-most-impact
Paul, II J. (1991). Lettera enciclica centesimus annus, 2004. Retrieved from http://w2.vatican.va/content/john-paul-ii/it/encyclicals/documents/hf_jp-ii_enc_01051991_centesimus-annus.html
Pearl, B. (2011). Britta Riley: A garden in my apartment. Retrieved from http://opensource.com/life/11/12/britta-riley-garden-my-apartment
Potter, D. (2014). Why the future of social innovation is open. *Stanford Social Innovation Review.* Retrieved from https://ssir.org/articles/entry/why_the_future_of_social_innovation_is_open
Rayner, T. (2011). The coalition of the willing. Retrieved from http://coalitionofthewilling.org.uk/
Seforis Consortium. (2013). The state of social entrepreneurship, key facts and figures. Retrieved from http://www.seforis.eu/upload/reports/1._Key_Facts_and_Figures_of_Social_Entrepreneurship.pdf
Svendsen, A. (1998). *The stakeholder strategy: Profiting from collaborative business relationships*. San Francisco: Berrett-Koehler Publishers, Inc.

Vodafone Corporate Social Responsibility Report 2014. Retrieved from https://www.vodafone.com/content/sustainability/our_vision_and_approach/managing_sustainability/stakeholder_engagement.html

Wren Montgomery A. (2012). "Collective Social Entrepreneurship: Collaboratively Shaping Social Good" Article in Journal of Business Ethics 111(3).

Second-Order Science and New Cybernetics 30

Karl H. Müller

Contents

Abstract

Currently, the global science system undergoes an epochal transformation which can be summarized as a transition from It-Science to Bit-Science. Bit-Science, as a new phase in the evolution of science, has brought about fundamental changes in scientific production processes, significant reconfigurations in the architecture of science, new organizations of research designs, and complex interaction patterns with the societal and natural environments of science. The great transformation from It-Science to Bit-Science can be summarized as a dual revolution in complexity and reflexivity. The emergence of second-order science becomes by far the most significant change for the rise in reflexivity dimensions of the overall science system. In view of these fundamental transformations of the science system, a new type of cybernetics can be developed under the name of "new cybernetics," which supersedes the area of traditional or first-order cybernetics, introduced by Norbert Wiener and second-order cybernetics, constructed as a new reflexive version of cybernetics since the late 1960s with its emphasis on observing systems, goals, and observers. The second part of this article explores

K. H. Müller (✉)
Steinbeis Transfer Center New Cybernetics, Vienna, Austria
e-mail: khm@chello.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_15

the new cognitive horizons of new cybernetics as well as its central goals, functions, and tasks. New cybernetics becomes a unique domain with a maximum degree of reflexivity for the science system in general.

Keywords
Second-order science · Methodology of science · Democratization · Reflexivity · Knowledge society · Cybernetics · Turing societies

Introduction

This article addresses major changes and transformations in the general science system that were summarized, so far, in terms of Mode 1 and Mode 2 (Gibbons et al. 1994; Nowotny et al. 2001) and Science 1.0 and Science 2.0 (Nentwich and König 2012; Nielsen 2011; Waldorp 2008), as a phase transition from Science I to Science II (Hollingsworth and Müller 2008; Müller 2012; Müller and Toš 2012), as postnormal science (Funtowicz and Ravetz 1993, 2001), or as an expansion of helices from a single or double helix configuration of universities and government to a triple (Etzkowitz 2003; Etzkowitz and Leydesdorff 1998, 2003; Leydesdorff 2006), quadruple, or quintuple formation (Carayannis and Campbell 2009, 2010). Here, the various aspects of fundamental transitions will be summarized and integrated as a great transformation from It-Science to Bit-Science. It-Science was the dominant form of scientific production with a specific cognitive architecture, methodology, and epistemic mode from the emergence of modern science during the sixteenth and seventeenth centuries up to the decades from 1900 to 1950. The recent stage of Bit-Science can be characterized as an epochal change (Nordman et al. 2011) and a gradual substitution of the traditional ways of scientific world-making to new forms and frames across all major aspects and dimensions of former It-Science.

Cybernetics as a scientific field of investigation started during the 1940s as one of the several transdisciplinary research programs along with systems theory or artificial intelligence with a focus on information and communication technologies, circularities, feedbacks, goals, and control. Cybernetics gained stronger popularity in Eastern Europe and in the former Soviet Union (Gerovitch 2002), but was hardly institutionalized in Western Europe or in the United States. From the late 1960s onward, cybernetics was propagated under the new label of second-order cybernetics, but could not succeed in creating either university departments or research centers, especially after the closing of Heinz von Foerster's Biological Computer Laboratory (BCL) in the years between 1970 and 1976 (Müller and Müller 2007).

This article will provide a short sketch of the main features of the new stage of Bit-science with respect to production processes, cognitive architectures, and other dimensions, with a special emphasis on second-order science as a generalized form of reflexive research across all traditional disciplines and fields. Moreover, this article will open new cognitive perspectives and horizons for cybernetics in the form of "new cybernetics." Second-order science and new cybernetics can be viewed as a new stage in the evolution of science with high degrees of reflexivity

and powerful instruments for a more participatory and more democratic organization of science. Bit-Science becomes the central feature of contemporary knowledge or, alternatively, of today's Turing societies (Müller 2016).

From It-Science to Bit-Science

Following John Archibald Wheeler's famous phrase "It from Bit" (Wheeler 1990) or, alternatively, Julian Barbour's reverse aphorism "Bit from It" (Barbour 2011), It-Science was based on material or physical objects and on local analogue devices, whereas Bit-Science is focused on machine-coded bit-objects and digital devices and networks. It-Science differs from Bit-Science in at least four clusters of science dimensions.

The first group of fundamental changes between It-Science and Bit-Science lies in the production processes of science which were transformed far beyond expectations, given the long-term predictions for computers and their potential impacts (Kahn and Wiener 1967). These radical and nonlinear changes and innovations (Müller 2013b, c) occurred in the institutional science environments, in the home offices, and in private studies from local real-time writing processes with paper, pen, or, in later times, typewriters and a limited local information support in the form of personal libraries and locally available documents to a global virtual production process in cyberspace with access to a global digital knowledge base. The laboratories of traditional scientific work were concentrated in universities and research institutes and entirely embedded in an It-world of letters, papers, books, etc. The contemporary laboratories in science are fully embedded in a Bit-world from writing scientific papers to the underlying knowledge base, which can be accessed from nearly everywhere.

During the period of It-Science, access to relevant scientific knowledge was highly centralized and reserved for a few places worldwide in which universities, research institutes, or institutions of higher learning with very-large scale libraries were concentrated. Libraries were and can be classified as the empirical carriers of the scientific knowledge base during the period of It-Science. Outside these small centers, access to scientific knowledge was poor or, in most instances, not available. This deep split between small centers and wide peripheries was completely eliminated through the rapid diffusion of the global web.

Likewise, the potential for scientific cooperation shifted dramatically from face-to-face interactions and letters during the stage of It-Science to the new worlds of social media. Science 2.0 (Shneiderman 2008) can be viewed as a recent transformation in the forms of cooperations during scientific production processes. Science 2.0 addresses the growing potential for scientific interactions with the tools and instruments of Web 2.0. Ben Shneiderman sees in Science 2.0 a new era of disciplinary, inter- and transdisciplinary cooperations:

> Successful scientific collaboratories among genomic researchers, engineering innovations through open-source software, and community-based participation in cultural heritage

> projects are all early indicators of the transformative nature of collaboration. (Shneiderman 2008, p. 1349)

For Shneiderman, Science 1.0 refers to the traditional forms of network building, face-to-face interactions, cooperations, and exchanges from the beginnings of modern science up to the end of the twentieth century. Science 2.0 emerges currently and changes scientific production, interaction, and cooperation processes from its traditional local and face-to-face formats to new space-independent global forms. Additionally, Science 2.0 should also boost inter- and transdisciplinary communication and cooperation, due to the open access to materials by other researchers, to an easy cross-border entrance without the usual disciplinary barriers and to user-friendly web-formats and web-based research infrastructures.

An additional dimension of Science 2.0 refers to new methods and tools for the study of web-based sociotechnical systems and their dynamics. In situations like natural disasters, communication and coordination processes become central for successful relief operations. Within this context, Science 2.0 can provide the necessary web-support for organizing these communication and coordination processes. At the same time, researchers obtain in the case of a natural disaster the necessary data to study and analyze the dynamics of these processes.

Additionally, Bit-Science is characterized by a differentiation in science levels into a zero-order, a first-order, and a second-order level and three corresponding types of science, namely zero-order, first-order, and second-order science (Riegler and Müller 2014; Malnar and Müller 2015; Müller 2016).

- The zero-order level is reserved for the rapidly expanding domain of research infrastructures (see, for example, ESFRI (2006, 2008, 2011)) which, due to their contemporary scope and their functions for scientific research across all major disciplines, constitute a scientific level *sui generis*.
- The first-order level continues to be the level for scientific explorations of nature, society technology, and the possible worlds of logic, mathematics, and other normative fields as well as the production center for models, methods, mechanisms, theories, experiments, axiomatizations, formalizations, or technological systems.
- Finally, the second-order level, like the zero-order level, extends to all major disciplines and fields and has its focus on in-depth investigations of components from first-order science.

Likewise three types of science can be specified for each of these three levels as well.

- Zero-order science comprises the expansion, the advancement, the interoperability, and the maintenance of research infrastructures (Dusa et al. 2014; Kleiner et al. 2013).
- First-order science can be classified like in the centuries before as the mode of exploring the world.

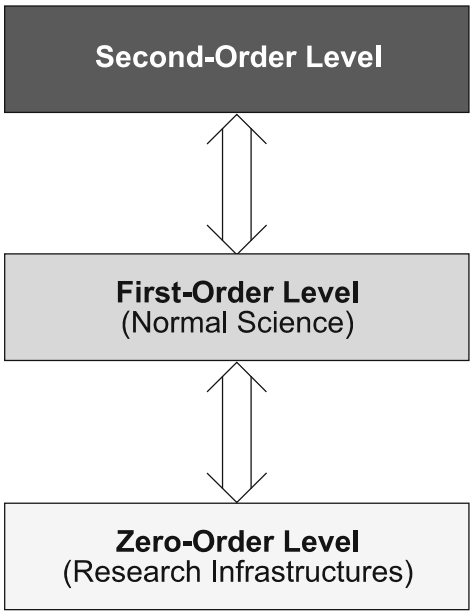


Fig. 1 The new three-level configuration of Bit-Science (The figures in this article were produced by Michael Eigner and Armin Reautschnig)

- Second-order science operates and works on elements from first-order science. More specifically, second-order science deals with building blocks from first-order science, both on its input side and output side where these building blocks are analyzed with operations like ordering, deepening, heightening, integrating, or widening in manifold ways.

Figure 1 presents this new level differentiation for Bit-Science where these three levels become strongly interlinked.

The general architecture of science undergoes deep transformations as well, which have been summarized under the name of Science II (Hollingsworth and Müller 2008). These changes are based on two principal components, namely complexity (Hayek 1967, 1972) and reflexivity (Umpleby 2010a, b), where each of these components comprises several science dimensions (Müller 2016).

This concludes a very brief sketch on the current great transformation from It-Science to Bit-Science with respect to production processes and science architecture.

The Rise of Second-Order Science

This section presents the main characteristics of second-order science which emerged in the last decades of the twentieth century. More specifically, second-order science arose in a mode of scientific self-organization to cope with the exorbitant volume of published scientific materials worldwide. A new research design was created under the name of meta-analysis for the rapidly growing number

of studies, tests, results, and the like, which used similar or identical designs, approaches, or explanatory schemes which differed only in time, space, and in research groups from one another. The concept of meta-analysis was first proposed by Gene V. Glass, an educational scientist, in the year 1976. Glass distinguished between primary and secondary data analysis on the one hand and meta-analysis on the other hand where he described a meta-analysis as a collection of all relevant studies on a highly comparable or identical topic and as a systematic analysis of the data pool of these studies. Glass introduced meta-analysis as

> the analysis of analysis and as a statistical analysis of a large collection of analysis results from individual studies for the purpose of integrating the findings. It connotes a rigorous alternative to the casual, narrative discussions of research studies which typify our attempts to make sense of the rapidly expanding research literature. (Glass 1976, p. 3)

Table 1 shows that meta-analyses in psychology, for example, were practically absent during the 1960s and emerged 1 year after the publication of Gene V. Glass' article, albeit in a minimal version. By the mid-1980s, however, meta-analyses turned out to be more frequent (see, for example, Glass et al. (1981), Hedges and Olkin (1985), Hunt (1999), Hunter and Schmidt (1990)) and from the 1990s onward, meta-analyses became an established research field within psychology, the social sciences (Wagner and Weiß 2014), clinical research, economics, business administration, and many other areas. Additionally, meta-analyses, due to their large and growing numbers in comparable fields, became objects for meta-meta-analyses and this process can continue, in principle, to even higher levels.

From the 1980s onward, more and more statistical methods and tools were developed which dealt with biases of all sorts of spurious effects. The four important characteristics of meta-analyses lie in the following points.

- Meta-analyses are based on a large number of available, directly comparable, and mostly quantitative studies.
- Additionally, meta-analyses are performed with partly new statistical methods and tools which were especially designed and developed for pooled data sets

Table 1 "Meta-analysis" as keyword in psychological abstracts

Year	Number of counts
1967–1976	0
1977	2
1978	4
1979	6
1980	9
1981	18
1982	32
1983	55
1984	63

Source: Hunter and Schmidt 1990, p. 40

(see, for example, Borenstein et al. (2009), Card (2012), Welton et al. (2012), or Whitehead (2002)).
- Moreover, meta-analyses moved out of their initial domains in psychology, medical research, or education science and spread over practically all major science fields and disciplines, including the life sciences or theoretical physics.
- Finally, the prefix "meta" has acquired very different meanings when applied to science domains. In areas like metalogic or metamathematics, the prefix "meta" indicates foundational issues both for logic and for mathematics, whereas metapsychology or metabiology designates special fields within biology or psychology. Metabiology, for example, can be considered as a recombination between genetics and algorithmic information theory (Chaitin 2009), and metapsychology has a clear focus on a client-centered setting with a strong emphasis on traumatic stress syndromes (Gerbode 2013).

Partly for these ambiguities and partly for the need of a three-level differentiation of the science system, the new terms of second-order level and second-order science were chosen instead of the concepts of metalevel and combinations between "meta" and scientific disciplines or fields. Still, meta-analysis can be viewed as the avant-garde for second-order science in the late twentieth century. But second-order science transcends meta-analyses in multiple ways and dimensions. Here, only three points will be mentioned.

- First, second-order studies can and must create their own data bases and are not restricted to available data from studies, tests, etc. A comparative second-order investigation on utilization patterns of big European surveys like the European Social Survey (ESS), the Survey of Health, Ageing and Retirement in Europe (SHARE), and the European Value Survey (EVS), while desirable and even necessary, requires a long period of data collection and documentation work of approximately 2 years for a group of three researchers. Thus, second-order studies are no ready-mades with respect to their necessary data base.
- Second, second-order analyses can be undertaken with input or output elements from first-order science and are not restricted to the output-side alone. This point becomes especially relevant for input elements like theories, explanations, models, or generative mechanisms where a second-order analysis requires more general, more integrated, or deeper theories, explanations, models, or generative mechanisms.
- Third, a particularly striking difference lies in academic disciplines and fields as elements of second-order science like second-order sociology, second-order political science, or second-order life sciences. In principle, second-order science comprises as many fields or disciplines as first-order science (correspondence principle).

Thus, second-order science needs a big jump from the area of meta-analysis to the more general spheres of a second-order level and of second-order analyses in their fully developed potentials. To show these rich potentials of second-order science, a

particular field of first-order research will be selected for this article, namely social survey research, which can be empowered with new perspectives from second-order survey studies (Malnar and Müller 2015).

Second-order science is based on three different groups or clusters of operations, and its general sequence of operations can be characterized as CAT-methodology with the three main steps of

- Choice of a specific second-order problem, collections of relevant building blocks from first-order science, and ordering these elements
- Analyses of these ordered and organized data base in various forms
- Transfers to first-order science

The first general C-step in the general methodology of second-order studies requires itself three basic operations. The first one is a re-entry operation RE, which was originally suggested by George Spencer-Brown (1969). Re-entries constitute the first step toward the vast open frontiers of second-order science. The operation of re-entry occurs whenever elements or building blocks from first-order science are applied to themselves in the form of

> computation of computation, cybernetics of cybernetics, geometry of geometry, linguistics of linguistics, logic of logic, magic of magic, mathematics of mathematics, pattern of pattern, teaching of teaching, will of will. (Kauffman 2005, p. 129)

This list can be extended, following Heinz von Foerster, with "understanding understanding," "communication of communication," "goals of goals," "control of control," etc. Usually, these self-referential twists through re-entries are considered as a playful field or pastime for logicians, mathematicians, or philosophers. Here, they become the basis for building a vast new science landscape.

The building blocks for second-order science are not necessarily only concepts or processes (e.g., "understanding understanding") but also theories, models, and even entire disciplines. In a more formal way, a first-order science building block X with a re-entry operation RE produces X(X).

$$X \rightarrow [RE] \rightarrow X(X)$$

These re-entries can be undertaken in basically two different types.

- The first type is highly concentrated on a small domain from first-order science only.
- The second type of re-entries uses a wide array from first-order science fields and creates a special postdisciplinary topic at the second-order level where postdisciplinarity refers to a combination of transdisciplinary first-order composition and second-order analyses (Müller 2016).

With respect to a second-order study of social survey research, many ways are open from the input side to the output side. As an empirical example, a big empirical

second-order study of the European Social Survey (ESS) can be specified as an ESS-study X of ESS-studies as follows:

$$X \rightarrow [RE] \rightarrow X(X)$$

where a second-order ESS-analysis X(X) is based on past and present studies which use the ESS as their data base (X).

The next step with respect to the first stage of choosing a problem and collecting relevant materials from first-order science lies in multiple adding operations in order to generate a rich variety of different cases, instances, or examples of a particular building block X(X). Even if second-order science is focused on a single concept from first-order science, the investigations are always undertaken with a large number of different instances or versions of this particular concept as it is used in first-order science. Thus, second-order science is bound to work permanently on multiple building blocks from first-order science simultaneously. Like evolutionary population dynamics, second-order science has to be organized as an investigation of groups or multiple groups of building blocks from first-order science.

Thus, selecting first-order building blocks like concepts, theories, models, methods, test results, functions, or generative mechanisms becomes the second step for research problems and research in second-order science.

In general, re-entries plus addings constitute a new science domain *sui generis* whose potential was not sufficiently recognized and only very insufficiently explored so far (Müller and Riegler 2014). What has been mostly disregarded until now is the relevance of these re-entries and addings for the creation or production of new scientific areas of investigation. Obviously, these re-entries and addings can be undertaken within all scientific disciplines and subdisciplines of the first-order level. In principle, a vast number of new second-order research problems are distributed across the same range of scientific disciplines and subdisciplines which are used for the first-order level. Three examples for re-entries and addings will be presented to demonstrate their generative power for second-order research.

- The first example focuses on theoretical concepts in sociology like living conditions, quality of life, or social capital. Usually, a large number of different versions can be found with respect to the operationalization of these concepts. By producing a re-entry into these concepts plus an adding operation of assembling these different specifications for these theoretical terms, one has created a suitable basis for comprehensive second-order investigations which can be undertaken into various directions.
- The second and highly postdisciplinary example is concentrated on a specific type of distribution which runs under the name of power-law distributions (Newman 2005; Newman et al. 2006) and which becomes relevant for a large class of scientific disciplines (Kajfež-Bogataj et al. 2010). As one among many possible directions, these power-law distributions and their underlying generative mechanisms can be transformed into a second-order study of generative mechanisms for power-law distributions. Here, the emphasis changes to a deep search for more

general generative mechanisms which are able to generate different types of generative mechanisms (see, for example, Helbing (1993) or Sornette (2006)).
- As a third example, the second-order ESS-study collected almost 3000 articles across different science disciplines which used data from the ESS so far (Malnar and Müller 2015). These articles constitute the relevant data base which needs further documentation steps for subsequent in-depth analyses.

Obviously, these three examples of re-entries in different areas of first-order science cover just a tiny fraction of possible re-entries. Currently, more and more first-order disciplines and fields are creating their corresponding second-order domains. In psychology and clinical research, for example, the studies of studies or the tests of tests abound which became powerful tools to strengthen or to disconfirm studies or tests undertaken at the first-order level. Basically, each scientific field or discipline is currently building its own second-order domains by applying their research results and studies, etc., to second-order investigations.

The third operation within the first stage of the CAT-methodology is rather obvious because what is needed at this point is an ordering of the various building blocks according to a small set of order parameters. These order-parameters rearrange the first-order building blocks and place them in comprehensive schemes or data bases. The specification of these order-parameters is highly dependent on the second-order issue, the available first-order building blocks, and the goals of analysis. In the case of the second-order ESS-analysis (Malnar and Müller 2015), the following order-parameters or criteria were chosen which provide basic information on the scope and the organization of first-order analyses with ESS-data. Here, an intensive documentation for each of these articles was produced in which each article was classified according to a large number of criteria or order-parameters.

- Type of publication: The first-order parameter distinguishes between various types of publication like a journal article, a book or a book chapter, a conference paper, a research report, and the like.
- Relevant discipline(s) for journal publications: In case of journal publications, the academic disciplines most relevant for a journal are to be documented.
- Language of publication.
- Country affiliation of first listed author.
- Number of authors.
- Main ESS-domain(s): The ESS-survey is divided into several larger segments like politics, citizenship, government, immigration and nationality, inequality, and the like, which are documented for each publication.
- Specific topics and ESS-variables: Each of the main ESS-domains was separated into a small number of indicators or variables and this order parameter determines the specific ESS-variables used in a publication.
- ESS-rounds used for the analysis: The ESS is organized in 2-year intervals and this criterion specifies whether an ESS-analysis focuses on a single round, on two, or on more rounds, or on all rounds so far.

- Keywords: Here, the keywords listed in a publication are reproduced and each article was documented with keywords from the side of the second-order investigator.
- Methods of data analysis: This order parameter specifies the type of data analysis, ranging from basic statistics to more advanced methods like cluster or factor analysis up to multilevel modeling.
- Intensity of data usage: This order parameter differentiates between varying degrees of dependence on ESS-data, ranging from an exclusive reliance of ESS-data to only a marginal usage of ESS-data, compared to other data sources.
- Other European data sources: Finally, the last criterion refers to other European data source like the International Social Science Program (ISSP), the European Value Survey (EVS), or the World Value Survey (WVS) and specifies the inclusion of these other data sets in a given publication.

With these parameters, the available first-order ESS-articles could be rearranged in a large data base which was to become the focus for subsequent investigations.

Following the C-phase of choosing a problem, collecting relevant elements from first-order science, and cataloguing them, the next general A-stage leads to analyses in second-order science and requires, once again, several operations.

The first step requires an in-depth analysis which is capable of entailing all major building blocks from the ordered empirical base. This step is, once again, very much dependent on the goals, on the type of first-order building blocks, and on the ordering operation.

- With respect to the second-order ESS-analysis, the major work lies in an in-depth investigation of the rich data base and in statistical analyses of this data base. Here, three different empirical profiles for ESS-utilization, for users, and for publications could be generated, which offered a large number of new and surprising insights like a highly specific use of the available ESS-data base with a focus on a small number of ESS-core variables.
- Additional steps can be added like the construction of appropriate models or theories for the results of the second-order analyses so far and the advancement of explanatory second-order accounts. Moreover, deeper or higher accounts of explanatory schemes, model, or generative mechanisms can be pursued which are capable of producing the available first-order accounts.
- The final T-stage of the CAT-methodology adds an important element especially for the relations between second- and first-order science. In this part of analysis, the transfer elements of second-order investigations and their effects and impact on first-order research are to be discussed in greater detail. In general, a large number of outputs of second-order studies can be used by the respective fields of first-order science for new explorations. In the simplest instances, second-order studies question the effects of medical drugs, based on a large number of first-order clinical studies, or the validity and reliability of psychological tests, again on the basis of a large quantity of test procedures. In more sophisticated cases, a

second-order investigation produces new empirical insights which can be used by a variety of researchers across different fields, as will be shown immediately. Even more complex second-order outcomes in theory or model formations lead to further first-order explorations in areas of model and theory applications or model and theory testing.

- Turning to the example of the second-order analysis of ESS-articles, one can point out to a large number of effects not only for future ESS-data collection processes and for ESS-based research, but for different areas outside the domain of social comparative research as well.
- First, the ESS-coordinating team receives a new and highly valuable utilization profile of ESS-data sets which becomes relevant for subsequent rounds of ESS-surveys.
- Second, social researchers become familiar with the main thematic interests of their community. Moreover, the weakly analyzed parts of ESS-data offer the possibility to initiate new ESS-analyses. Furthermore, the range of available themes can be used for recombinations and for the creation of new ESS-topics, which then become the focus of analysis.
- Third, experts in the field of methods for social research get an overview of blind spots in terms of available methods of analysis. For example, a marginal number of articles can be found which use the entire spectrum of all available ESS-data from the six rounds so far. This provides a strong incentive to develop new dynamic tools of analysis which are specially constructed for a complete utilization of the ESS-data base across all rounds.
- Fourth, specialists in the sociology of science gain empirical data on the regional distribution of social research and on the thematic preferences of social researchers across time.
- Fifth, as the ESS-data production continues in its 2-years intervals, sociologists of knowledge will be able to work with a rich data base on shifts in thematic interests of European social researchers and relate these shifts to societal challenges and changes, economic and financial crises, and political debates in the public domain.
- Sixth, researchers in the area of embedded cognition are offered a rich data source on the interpretation of data by ESS-researchers and can use these findings for laboratory studies of interactions between survey interviewers and respondents.
- Seventh, groups responsible for European and national science policies receive permanent inputs on the status of European or national social science research across Europe or in a particular country.

Due to the variety of transfers within and outside the domain of social research, the example with a second-order ESS-analysis becomes a fascinating instance that a second-order analysis in a seemingly narrow domain can generate results for a much wider variety of first-order fields. Moreover, first-order survey research can be empowered with second-order survey research as a reflexive domain for quality control and for innovations which is capable of energizing first-order investigations with new inputs and horizons.

These three general stages comprise, in essence, the basic CAT-specifications for a fully developed general second-order methodology across all scientific areas from logic and mathematics to the natural or to the social sciences.

In the past and even in the present times, first-order science worked and operates seemingly well, productively and innovative. So what makes research in second-order science so important and relevant, if not outright indispensable? Here, a final argument can be developed why second-order research becomes more and more necessary as the evolution of the overall science system continues.

A first hint for answering this question can be found in the work of Ulrich Beck (1986, 2000, 2007) and in his analysis of reflexive or self-infective effects of science and technology. First-order science can no longer offer itself as a natural cure if at least parts of the new societal problems are due to an involvement of scientific procedures and outputs in the first place. Second-order science can address these problems of systemic failures in the implementation of science-based policies or technological systems in a new way which is based on a large quantity of case studies and overviews from science studies, which can be analyzed and systematized further with the tools and instruments from second-order science.

But aside from Beck's self-infective configuration and the necessity for in-depth second-order studies, another argument can be put forward of an inversion of novelty. This inversion of novelty assumes a shift in the sources of scientific inventions, innovations, and radical breakthroughs (Hollingsworth and Hollingsworth 2011) from the dominant mode of exploring the world to the reflexive mode of focusing of the already available scientific outputs, resources, publications, and the like. Moreover, this inversion of novelty should have significant implications also for science policy and for teaching or curricula developments. Figure 2 captures several of the characteristic elements of this novelty inversion with a focus on the social sciences.

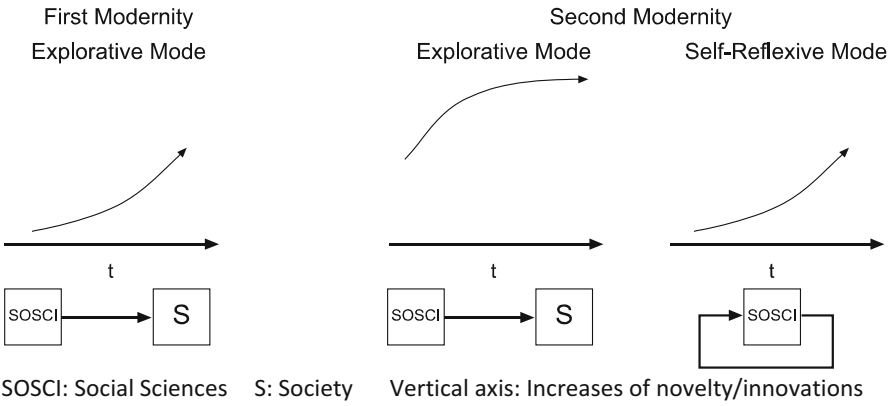


Fig. 2 An inversion of novelty in the social sciences within contemporary and future science landscapes

On the left-hand side of Fig. 2, one can see the expansion of the social sciences in their explorative mode on the social and societal worlds which is represented by the lower half of an S-shaped curve with high increases in novelty or social science innovations.

The inversion of novelty comes about in the right-hand part of Fig. 2, which shows that novelty in the social sciences is based to a diminishing extent on the advances of explorative social sciences, on the exploration of new topics and domains, or on the construction of new models or theories. Rather, high levels of novelty and innovation in the social sciences occur in reflexive analyses of already completed social science elements like theoretical concepts, models, or publications.

This inversion of novelty can be supported with the help of two examples from different domains, again taken from the social sciences.

- First, with respect to theoretical concepts in the social sciences like standards of living or quality of life, it becomes more and more difficult, due to a rich variety of already available versions, to produce significant new insights through adding another version for these two already very diversified concepts. However, an investigation on the available versions of these two concepts should produce new insights on the scope and on the main domains of these two theoretical terms, on robust relations between different segments or aspects of standards of living and quality of life, or on their mutual dynamics. Additionally, these reflexive investigations can be extended to a study on the scope of living conditions and on quality of life combined which will produce, in all probability, new insights into the differences and similarities between these two concepts (see also Müller 2013a, b).
- Second, evaluating, for example, a specific ensemble like a university, an academy of science, or a national system of innovation for the nth time will produce, in all probability, less innovative content than a reflexive investigation of the n−1 evaluation reports so far and of their relations to the overall societal dynamics, including political changes. Moreover, a rich variety of different reflexive evaluation designs can be implemented, in principle, so that the outputs of these reflexive evaluation studies on already available evaluations are capable of producing significantly higher degrees of novelty than a renewed analysis, given the already available results of previous evaluations.

As time goes by, the accumulation of more and more studies, articles, or results in first-order science should strengthen and intensify the assumption of an inversion of novelty, which is not only limited to the social sciences but to the science system in general. This, in turn, would imply that reflexive research changes, in due course, from a strange and peripheral issue to a sheer necessity for the contemporary or the future global science system as a whole.

Additionally, second-order science can advance to higher orders, starting from order 1 and second-order studies of building blocks from first-order science, to order 2, which comprises second-order studies of second-order studies, to order 3, with a focus on second-order analyses of second-order analyses of order 2, to order

Table 2 Two primary goals for second-order science

Goal set I: quality control	Goal set II: innovation
Quality improvements of first-order building blocks (robustness)	New inputs for first-order science with high comparative advantages (generality, depth, integration, height, etc.)
Quality attributions of first-order building blocks as empirically inadequate/nonviable general quality assessments	New research fields; new perspectives and cognitive horizons; empowering first-order fields and disciplines

4, which is concentrated on second-order research of second-order studies of order 3, to order 5, and so on. Thus, second-order science is capable to cope with a large accumulation of second-order investigations and to open new scientific frontiers for second-order research at higher orders.

Finally, science–society relations have become highly complex in the transition from It-Science to Bit-Science. At this point, it must be sufficient to point out to various conceptions of a triple, quadruple, and quintuple helix (Carayannis and Campbell 2009, 2010) which offer a rich conceptual framework to analyze these new configurations.

Moreover, second-order science fulfills two main goal sets for the overall science system, namely quality control and innovation, which are summarized in Table 2. The first set of quality control operates especially on outputs of first-order science, whereas the second goal set of innovation addresses the effects of second-order research for first-order science.

Concluding the first part of this article, Table 3 summarizes the main differences between It-Science and Bit-Science which were presented so far.

With Table 3 the brief summary of a great transformation in science from It-Science to Bit-Science and of the vital role of second-order science in this transition comes to an end. This great transformation can be classified also, due to its depth, scope, and the exchange of center–periphery relations, as a dual revolution in complexity and in reflexivity dimensions for the overall science system or as a second Copernican revolution, after the first Copernican revolution by Nicolaus Copernicus and his center–periphery inversions between the earth and the sun.

The Three Stages of Cybernetics from the 1940s Onward

Shifting to the second concept in the title of this article, new cybernetics can be linked to the unfolding of second-order science in a strong, circular, and coevolutionary manner where second-order science provides a positive impact for the rise of new cybernetics and, in turn, new cybernetics is capable of empowering second-order science.

Originally, the term κυβερνήτης (*kybernētēs*) meant “steersman, governor, pilot, or rudder” and comprised both the object for navigation as well as the person responsible for steering. A cybernetic configuration, according to Fig. 3, involves an assembly of at least seven components which have to be present simultaneously.

Table 3 The main differences between It-Science and Bit-Science

	It-Science (traditional science from the sixteenth century to 1900/1950)	Bit-Science (new stage from 1900/1950 onward)
Production processes		
Knowledge base	Local, highly centralized	Globally distributed, loss of peripheries
Workspaces	It-based	Bit-based, cyber, virtual
Cooperation	Science 1.0	Science 2.0
Science architecture		
Levels	Single level	Differentiation into three levels
Complexity	Low	High
Reflexivity	Low	High
Institutionalization of reflexivity	-	Second-order science
Orders of reflexivity	-	Second-order science of higher orders
Research designs/fields		
Epistemic mode	Exo-mode[a]	Endo-mode[a]
Problem solution	Theoretical problem solutions	Theoretical/practical problem solutions[a]
Cybernetics	First-order cybernetics	New cybernetics
Science–environment relations		
Composition	Single/double helix (science–government)	Quintuple helix (science–government–industry–media–environment)

[a]These concepts will be described in the following section

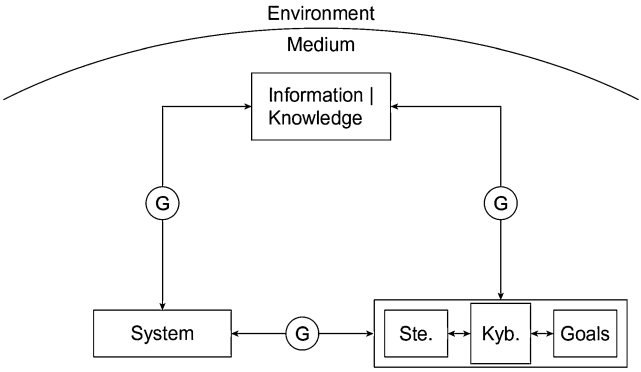


Fig. 3 The cybernetic configuration. *Ste* Objects of Steering and Control, *Kyb* Kybernētēs, Steersman, Navigator, *G* Generative Relations

- First, a steersman (Kyb.) or an operator is required as the main actor for navigation. Steersmanship can be performed by humans, but also by machines like in the case of an autopilot, by robots, or by animals.
- Second, objects of steering, control, or navigating (Ste.) are needed like a steering wheel, a rudder, or other mechanical or physical devices for steering and control.
- Third, the goals of the steersman or operator become another necessary ingredient in the cybernetic configuration, responsible for dynamic aspects of drifting and navigating.
- Fourth, an operating system for the steersman and her or his steering instruments must be available. These navigating systems can be as diverse as boats, vessels, planes, cars, trains, busses, undergrounds, etc.
- Fifth, a medium of navigation must be specified. The medium can be qualified as the immediate or surrounding environment in which steering and navigating takes place like the sea, a river, the air, roads, tracks, or land.
- Sixth, the cybernetic configuration needs a constant flow of signals, measurements, and information as well as a knowledge base in order to determine the directions and deviations of the operating system and the goals.
- Seventh, the steersman, her or his navigating system, and the medium operate within a wider environment, which places additional constraints, barriers, or options for navigating and movements.

Obviously, these components must be interlinked with multiple feedback and feedforward processes and organized in a circular and triadic way. Such a triadic configuration with three basic nodes is organized in generative relations G which differ from causal relations in terms of mutual (re)-production and stability. In a triadic formation with generative relations, each node produces and reproduces itself as well as the others in a never-ending loop and as long as the triadic ensemble persists.

The cybernetic configuration can be represented through Fig. 3 in which all seven necessary elements become assembled and interlinked with generative relations.

It is highly interesting to note that cybernetics was constructed so far in three consecutive versions which followed a general drift toward higher levels of reflexivity. Each of the three cybernetic variants placed specific elements of Fig. 3 in its cognitive core. Thus, new cybernetics as the currently third variation of the cybernetic configuration is built and developed with specific tasks and functions for second-order science.

Cybernetics as a scientific field of inquiry started during the 1940s through the annual meetings of a highly inter- or transdisciplinary group, which was supported by the Josiah Macy Jr. Foundation and which met in New York's Beekman Hotel. In the spirit of Norbert Wiener's book *Cybernetics* (1948), the science of cybernetics had initially a highly technical orientation which emphasized three components from the general cybernetic configuration, namely technical control systems, the objects, or instruments of control and information, as shown in Fig. 4. Cybernetics had a clear focus on information and communication technologies and on goal-directed machines and automata. W. Ross Ashby's (1954, 1956) homeostat became a classical cybernetic mechanism and the paradigm for self-regulation as well as the basis for Ashby's law of requisite variety. For its first phase, cybernetics can be described

> as a science based on the assumption of consonances between living organisms and machines. In cybernetics, humans, machines, and organizations are systems of communication and control . . . in the homeostatic or self-regulatory sense rather than in the coercive sense. (Light 2003, p. 37)

During the 1950s and 1960s, cybernetics was strongly linked to cybernation (Michael 1962) and automation and to the industrial military complex (Heims 1985, 1991). Cybernetics became especially strong in the Soviet Union, although 30 years later the two keywords of cybernation and automation were already

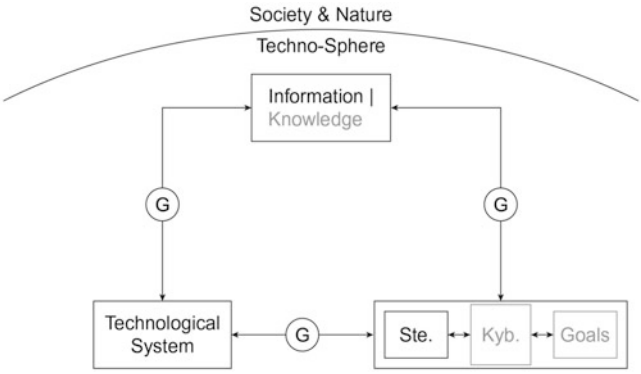


Fig. 4 Classical or first-order cybernetics. *Ste* Objects of Steering and Control, *Kyb* Kybernētēs, Steersman, Navigator, *G* Generative Relations

outdated. In John A. Barry's study on computers and technobabble (Barry 1991), for example, both automation and cybernation had disappeared from the hot spots of computer idioms.

From the late 1960s onward, two significant changes occurred, namely a shift to the steersman, governor, operator, or pilot on the one hand and a self-referential turn to cybernetics itself. Both turns used the name of second-order cybernetics which to this very day created a deep ambiguity on the status of second-order cybernetics. For example, the book cover of Heinz von Foerster's cybernetic encyclopedia from 1974 (Foerster 1974) has both different versions on it, namely cybernetics of cybernetics as its title and the definition of second-order cybernetics as the cybernetics of observing systems on its cover as well.

- The first turn was undertaken by Heinz von Foerster, Gordon Pask, Ranulph Glanville, Louis H. Kauffman, Bernard Scott, Stuart A. Umpleby, and others. The first version takes second-order cybernetics as the "cybernetics of observing systems" and differentiates it from first-order cybernetics as the "cybernetics of systems observed" (Foerster 1974). This turn can best be understood as an epistemic shift of world-making from the traditional mode "from without" to a new mode "from within," which will be discussed subsequently and which was included in Table 3 already as one of the major shifts from It-Science to Bit-Science.
- The second turn can be attributed to an interaction between Heinz von Foerster and Margaret Mead and is based on an episode in the year 1968 where the construct of "cybernetics of cybernetics" was born. Margaret Mead presented a lecture on the status of cybernetics with cybernetic means (Mead 1968); Heinz von Foerster had to search and find an appropriate title for this lecture in view of a long absence and silence on the part of Margaret Mead.

> So I had to edit her speech and invent a title. What struck me was her speaking about cybernetics in a cybernetical way. Thus I chose for her the title 'Cybernetics of Cybernetics' (Foerster 2003, p. 302).

From this short episode, one gets the impression that second-order cybernetics is mainly concerned with self-reference and with the application of concepts, methods, and theories onto themselves. But the second turn was not developed further toward a new science frontier like in the case of second-order science, to a stream of cybernetic analyses of cybernetics or to a special methodology for the analysis of self-referential concepts. Instead, perspectives of cybernetics of cybernetics, communication of communication, or control of control were compiled under the notion of autology, but without significant impacts either for cybernetics or for the science system in general.

Not surprisingly, second-order cybernetics or, alternatively, new cybernetics in its version of the 1980s and 1990s (Pask 1996; Van de Vijver 1992) was strongly associated and linked with the first turn, namely with the inclusion of observers and with a new methodology for scientific operations "from within." Figure 5 presents an overview of the first metamorphosis of cybernetics from first-order cybernetics to

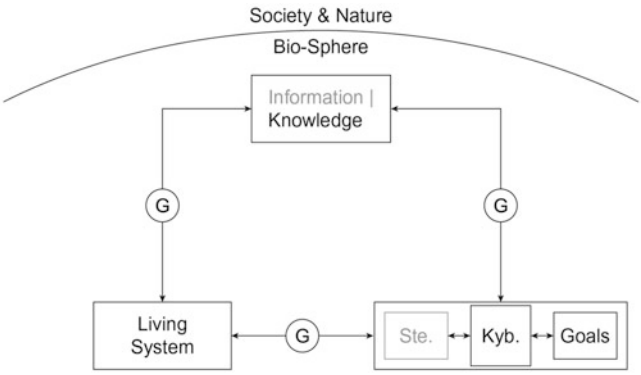


Fig. 5 An overview of second-order cybernetics. *Ste* Objects of Steering and Control, *Kyb* Kybernētēs, Steersman, Navigator, *G* Generative Relations

second-order cybernetics which followed along the first turn toward observing systems. This shift implied a strong emphasis on the goals of operators, navigating across living systems, and on knowledge and the scientific knowledge base, including rule systems of various sorts.

Second-order cybernetics as the cybernetics of observing systems advanced a new epistemic mode of scientific world-making and a new general methodology for scientific research. This new mode can be based on a new distinction and on a differentiation of the two concepts of an endo-mode and an exo-mode which represent two possible ways of exploring the world. Initially, it must be mentioned that Otto E. Rössler published a book on endo-physics (1992) which raised considerable interest (Atmanspacher and Dalenoort 1994). However, the distinction developed here between an exo-mode and an endo-mode differs significantly from the exo- and endo-differentiation by Otto E. Rössler who assumes a two-level structure of reality.

The distinction between an endo-mode and an exo-mode as a cybernetic invention can be traced back to Heinz von Foerster who developed a very intriguing list of characteristic differences between two fundamentally different epistemic attitudes toward one's world or environment.

> Am I an observer who stands outside and looks in as God-Heinz or am I part of the world, a fellow player, a fellow being? (Foerster 2014, p.128)

Subsequently, Heinz von Foerster provides a series of distinctions which can be used for the differentiation between an endo-mode and an exo-mode, where features like monological, denotative, "you say how it is," or schizoid belong to the exo-mode and characteristics like dialogical, connotative, "It is how you say it," or hominoid are included in the endo-set. For Heinz von Foerster, the decision between an exo-mode from without or an endo-mode from within belongs to the set of undecidable questions whose charm it is that they have to be decided by us.

This shift to the I of the observer or to the endo-mode requires profound methodological changes because, following Heinz von Foerster once again, "I am the observed

relation between myself and observing myself" (Foerster 2003, p. 257) and "I" invites a host of additional notions like self-reference, self-observing, self-reflexivity, and the like plus a long history of paradoxes, based on the notions of I and self. Over the past decades, George Spencer-Brown (1969), Heinz von Foerster (2003), Ranulph Glanville (2009, 2012, 2014), Louis H. Kauffman (1987, 2009, 2017), Bernard Scott (2011), or Stuart A. Umpleby (1991, 2007, 2016) offered the conceptual and logical foundations for consistent and nonparadoxical operations in an endo-mode.

Second-order cybernetics, due to its operations in recursively closed triadic configurations, can best be defined as the study of eigenforms and of the analysis of stable or invariant knowledge elements across first-order science (Kauffman 2017). The notion of eigenforms or eigenbehaviors was first introduced by Heinz von Foerster in a lecture on the occasion of Jean Piaget's 80th birthday in Geneva on June 29, 1976 (Foerster 2003, pp. 261–271). Due to closure theorem, eigenforms or eigenbehaviors can be described as the stable endpoints or, alternatively, as the invariants in recursively closed systems. "In every operationally closed system there arise eigenbehaviors" (Foerster 2003, p. 321). The endo-mode operates, following Louis H. Kauffman, in a reflexive domain in which eigenforms become the necessary endpoints of research processes by others as well as by second-order cyberneticians.

> The world of reflexive domains and their eigenforms is the world in which cybernetics occurs. (Kauffman 2017)

More specifically, Louis H. Kaufmann describes second-order cybernetics or, alternatively, endo-cybernetics in the following way.

> Cybernetics is the study of systems and processes that interact with themselves and produce themselves from themselves. This includes cybernetics itself as a system or process that interacts with itself and produces itself from itself. (Kauffman 2017)

For second-order cybernetics as endo-cybernetics and a focus on living systems, the new methodology from within implied also a search for hypotheses and laws of biology as eigenforms. Heinz von Foerster was very explicit that the laws of neuroscience and of biology, contrary to the laws of physics, have to be generated as eigenforms in a recursively closed procedure.

> The laws of physics, the so-called 'laws of nature', can be described by us. The laws of brain functions – or more generally – the laws of biology, must be written in such a way that the writing of these laws can be deducted from them, i.e., they have to write themselves. (Foerster 2003, p. 231)

Thus, eigenforms become the primary goal for the endo-mode especially in the study of living systems. In this way, second-order cybernetics created and promoted a drift toward the endo-mode as a new form of scientific world-making from within.

Table 4 presents the main goals and means for the exo-mode, which was the dominant mode during first-order cybernetics in particular and It-Science in general, and the new endo-mode, which was promoted heavily by Heinz von Foerster under the term of second-order cybernetics.

Table 4 Goals for the exo-mode and the endo-mode

	Goals	Means
Exo-mode (for zero-, first, and second-order science)	Objectivity	Eliminating observer effects, subjective biases, use of first-person language, etc.
	Truth and verisilimitude	Approximating true accounts
	Confirmation/corroboration and falsification	Eliminating erroneous building blocks; establishing empirical adequacy
	Value-freedom and neutrality	Eliminating evaluation biases
	Varieties of realisms (hypothetical, critical, scientific, messianic, scientific, myopic, etc.)	Producing new accounts for realism/empiricism as epistemic tradition
Endo-mode (for zero-, first, and second-order science)	I(Ob)-Inclusion in triadic and generative ensembles traceability of observers and reproducibility	I(Ob)-Integration; documentations of I(Ob)-operations; enabling the reproduction of scientific building blocks
	Viability	Constraints-assessments and establishing a consensus on the evolutionary adequacies of scientific building blocks
	Goal I(Ob)-specifications	Transparency of I(Ob)-goal-related components and their relations to outputs
	Eigenforms	Stable and robust results as the final outcomes of recursive interactions in triadic configurations or reflexive domains
	Varieties of constructivisms (radical, social, laboratory, phenomenology, first person science, etc.)	Producing new accounts for constructivism as epistemic tradition

Table 3 already indicated that the diffusion of an endo-mode should, is, and will be accompanied by a shift in scientific problem solutions and by a significant rise in practical problem solutions which are aimed at eliminating or significant reducing societal or environmental problems especially at the community level. The theoretical background for this type of problem solution goes back to the early stages of Bit-Science, although totally unrelated to the rise of digital information and communication technologies. During the 1960s and 1970s, a new approach under the name of action research (Burns 2007; Greenwood and Levin 2007; Noffke and Somekh 2009; Reason and Bradbury 2001) was propagated especially within Latin America (Fals Borda 1978). Since then, action research institutionalized itself especially in institutes or faculties for social work, in applied universities, or in institutes like the Institute of Cultural Affairs, a global NGO which started its operations in the year 1973 (Umpleby 2015). Table 5 presents an overview of the main differences between the dominant type of problem solutions throughout the period of It-Science and the new form.

Table 5 Two types of scientific problem solutions

Theoretical	Practical
Research problem RP	Societal/environmental problem SP
Building a theoretical/model framework for RP	Assessing SP (history, problem solutions in the past, target groups)
Collecting relevant data	Establishing a work plan
Theory/model-testing	Building a workforce for a solution of SP
Explanatory account for RP	Effective reduction or elimination of SP
Exo-mode (objectivity, observer-free, etc.)	Endo-mode
Success by publications and scientific impact	Success by improving the quality of life of target groups
Reliable theoretical knowledge	Robust practical knowledge

Table 6 Main differences between first-order cybernetics and second-order cybernetics

First-order cybernetics	Second-order cybernetics
Systems observed	Observing systems
Goals of systems	Goals of the observer
Observer excluded from research and research designs	Observer included in research and research designs
Self-reflexive research not admitted	Central relevance for self-reflexive research and for the study of eigenforms with a focus of living systems
Exo-mode (from without)	Endo-mode (from within)
Advancement of control capacities as its main goal	Advancement of methods, tools, and designs for participation and for consensus formations as its main goal

Under the old regime of It-Science, a research problem RP was solved once RP was successfully modeled, explained, and the theoretical problem solution allowed for additional features like forecasts or scenarios. Practical solutions require an effective reduction or elimination of a societal problem SP and this practical problem solution must have observable and positive consequences for the well-being or the quality of life of affected target groups or communities. Obviously, practical problem solutions will not replace scientific ones in the years ahead, but practical problem solutions should gain in relevance and should offer themselves as a viable alternative to a purely theoretical account of problem solving.

Finally, Table 6 presents some of the significant differences between second-order cybernetics as the cybernetics of observing systems and first-order cybernetics as cybernetics of systems observed. Again, the shift to an endo-mode and eigenforms become the characteristic new elements of second-order cybernetics compared to first-order cybernetics which operated still in the traditional exo-mode.

Ronald R. Kline (2015) makes the interesting observation that the cybernetic momentum was lost in the moment when cybernetics shifted to second-order

cybernetics which Kline considers as a failed attempt with no significant results and outcomes. So far, second-order cybernetics was only weakly developed and is concentrated in the works of a small circle of cyberneticians like Ranulph Glanville, Louis H. Kauffman, Bernard Scott, or Stuart A. Umpleby and of related research programs like the autopoietic program by Humberto R. Maturana, Francisco J. Varela, and Ricardo Uribe.

New Cybernetics: Its Main Goals, Functions, and Institutionalization Strategies

But a second metamorphosis of cybernetics is underway right now under the name of new cybernetics which differs significantly from new cybernetics as proposed, for example, by Gordon Pask. New cybernetics in its current and latest version encompasses, aside from the reflexive endo-mode of second-order cybernetics, also the second reflexive turn toward second-order science. Although Margaret Mead and Heinz von Foerster used the phrase of cybernetics of cybernetics, they did not view cybernetics of cybernetics or other autological terms like a sociology of sociology or a biology of biology as new research fields, which require also a specific methodology as it was introduced in this article. The second turn for new cybernetics was undertaken quite independently from second-order cybernetics by the overall science system itself and led to second-order science and its reflexive structure of

$$\mathrm{X} \rightarrow [\mathrm{RE}] \rightarrow \mathrm{X}(\mathrm{X}).$$

New cybernetics completes, thus, the reflexivity revolution, initiated by first-order and second-order cybernetics and focuses itself as one of its major tasks on the invariant eigenforms of the science system as a whole.

Aside from its operations in the endo-mode, new cybernetics brings a shift in the medium of navigation as well. With the second metamorphosis of cybernetics, the medium or domain of navigation changes from natural, social, and technical systems and from the level of first-order science to a new level of the science system, namely to the reflexive level of second-order science. Thus, the third stage in cybernetics is based on a second reflexive shift from first-order science to the reflexive level of second-order science as the medium for navigation.

Table 7 offers an overview of three types of cybernetics since its foundations in the 1940s, the failed version of cybernetics of cybernetics, and the dual reflexive movement or drift from the lower left corner, namely from first-order cybernetics as the starting point of a reflexivity revolution in science to the right upper corner of new cybernetics as its dually reflexive endpoint.

Thus, new cybernetics can be designed as a dual reflexive scientific field at the second-order level whose primary goal and function lies in the promotion of second-order science. This navigation can take three main pathways.

Table 7 Four fields of cybernetics from the 1940s onward

Epistemic dimension		
	Exo-mode (from without)	Endo-mode (reflexive, from within)
Second-order level (reflexive)	(Was never built and expanded as a new science frontier; based on Margaret Mead's 'Cybernetics of Cybernetics' from 1968)	New cybernetics dual reflexive field of research, central for the evolution of second-order science (from the 2010s onward)
Dimension of levels		
First-order level	First-order cybernetics (1940s – 1970s)	Second-order cybernetics, cybernetics of observing systems, endo-cybernetics, autology; from the late 1960s onward

- First, new cybernetics operates as an innovation pump especially for second-order science. New cybernetics produces new tools and instruments for second-order science as well as paradigmatic applications of these tools and instruments with a high innovative impact for first-order science. Moreover, new cybernetics works on special methodologies for specific second-order fields and specifies hot spots and research designs with strong effects for first-order research.
- Second, new cybernetics can and must pursue the path which was only weakly developed by second-order cybernetics, namely in-depth investigations of eigen-forms in their multiple aspects and in their wide variety.
- Third, new cybernetics can operate on second-order analyses of a higher order and specializes, thus, in second-order analyses of second-order analyses.

In this way, new cybernetics stays within the cybernetic configuration of Fig. 3 but offers new horizons for highly innovative and challenging research both for first-order and second-order science. In this manner, new endo-cybernetics becomes a reflexive science of science field with science as its reflexive domain.

Figure 6 presents the overall configuration for new cybernetics which has its new focus on second-order science and on the endo-mode as its standard way of conducting scientific research primarily at the second-order level.

The goals for second-order science were described already in the form of two goal sets, namely quality control and innovations. The goal sets for new cybernetics can be specified as quality control and innovations for second-order science itself. In particular, the following goals can be formulated for new cybernetics.

- A first target of new cybernetics lies in a formalization of the concept of robust knowledge and its identification and measurement since robustness becomes one of the characteristic comparative advantages of second-order studies. Additionally, new cybernetics should advance a general theory of viability which goes well beyond the viability descriptions provided by Ernst von Glasersfeld (1981).
- A second goal of new cybernetics lies in the construction of second-order studies of higher degrees across major disciplines and fields of second-order science

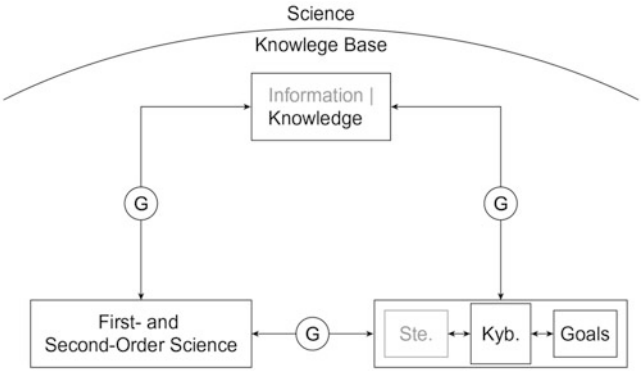


Fig. 6 The configuration of new cybernetics. *Ste* Objects of Steering and Control, *Kyb* Kybernētēs, Steersman, Navigator, *G* Generative Relations

where a second-order study of building blocks from first-order science can be classified as degree 1, a second-order study of elements from second-order science as degree 2, etc.

- A third highly self-reflexive objective of new cybernetics lies in the proliferation of second-order studies on scientific researchers and their operations. New cybernetics can offer second-order investigations on scientific observers, their operations, and emerging eigenforms across all major science fields and becomes, thus, a reflexive second-order field for the study of scientific observers. After its not-so-successful metamorphosis as second-order cybernetics, new cybernetics can become a second-order theory for scientific observers or researchers.
- A fourth goal of new cybernetics emphasizes the proliferation of new reflexive tools and instruments for second-order investigations, special second-order methodologies, and designs.
- A fifth goal of new cybernetics lies in the application and in testing these new tools and instruments which, additionally, can have a large impact for first- and second-order science.
- A sixth goal of new cybernetics lies in the monitoring of the evolution of second-order science and of new research topics and fields, based on the results of second-order science.
- Finally, a seventh aim of new cybernetics lies in a constant recombination of new cybernetics itself.

The function of new cybernetics can be qualified as reflexive for second-order science and for the science system in general, due to the goals specified above. Moreover, new cybernetics is capable of monitoring higher orders of second-order science and it can be qualified, thus, as a second-order domain which, by necessity, can reach the highest degree of order.

Table 8 Main differences between second-order cybernetics and new cybernetics

Second-order cybernetics (endo-mode, first-order level)	New cybernetics (endo-mode, second-order level)
Observing systems	Observing science
First-order research on first-order science	Second-order research on second-order science
Emphasis on eigenforms across first-order science	Emphasis on eigenforms across first-order and second-order science
Navigating in an endo-mode across first-order science	Navigating mainly across second-order science, but also across first-order science
Central for communication and coordination of first-order science	Central for communication and coordination of second-order science and for the science system in general

In terms of institutionalization, new cybernetics can become a PhD program which is organized in a self-similar manner to second-order science at the third cycle of the Qualifications Framework of the European Higher Education Area.

Table 8 provides a summary of the main differences between second-order cybernetics and new cybernetics.

Outlooks

New cybernetics was designed, linked, and embedded in a way so that it can develop and grow along with the expansion and diffusion of second-order science in a circular and coevolutionary manner. Moreover, first-order science, second-order science, and new cybernetics become organized in a generative triadic configuration where each node (re)-produces the other two and is (re)-produced by these two nodes at the same time. And due to the growing impact of research processes from within, the general science system across its three levels will advance the agenda of knowledge democracy worldwide.

In sum, the great transformation from It-Science to Bit-Science, a bit-based knowledge base, and a general shift to high levels of reflexivity have become the main ingredients of knowledge societies, present and future.

Moreover, new cybernetics has reached the endpoint of a long trajectory in reflexivity which began with first-order cybernetics as the starting point for bringing circularity, feedbacks, and reflexivity prominently into the science sphere, with second-order cybernetics and its construction of a new and reflexive way of scientific world-making and explorations and with new cybernetics as the unique science domain which becomes reflexive of reflexivity itself.

Finally, a short aphorism will conclude this article which emphasizes the recursive organization of first-order science, second-order science, and new cybernetics where, as one of many examples, new cybernetics produces new methods and designs which can be used by second-order science and applied on building blocks from first-order science which lead to new horizons and research paths for first-order science, *round and round*.

First-order science: The science of exploring the world.
Second-order science: The science of reflecting on these explorations.
New cybernetics: The science of reflecting on these reflections.

References

Ashby, W. R. (1954). *Design for a brain*. New York: Wiley.

Ashby, W. R. (1956). *An introduction to cybernetics*. London: Chapman & Hall.

Atmanspacher, H., & Dalenoort, G. J. (Eds.). (1994). *Inside versus outside. Endo- and exo-concepts of observation and knowledge in physics, philosophy and cognitive science*. Berlin: Springer.

Barbour, J. (2011). Bit from it. In A. Aguirre, B. Foster, & Z. Merali (Eds.), *It from bit or bit from it. On physics and information* (pp. 197–211). Heidelberg: Springer.

Barry, J. A. (1991). *Technobabble*. Cambridge: The MIT Press.

Beck, U. (1986). *Risikogesellschaft. Auf dem Weg in eine andere Moderne*. Frankfurt: Suhrkamp.

Beck, U. (2000). *World risk society*. Cambridge: Polity Press.

Beck, U. (2007). *Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit*. Frankfurt: Suhrkamp.

Borenstein, M., Hedges, L. V., Higgins, J. P. T., & Rothstein, H. (2009). *Introduction to meta-analysis*. Chichester: Wiley.

Burns, D. (2007). *Systemic action research: a strategy for whole system change*. Bristol: Policy Press.

Carayannis, E. G., & Campbell, D. F. (2009). 'Mode 3' and 'quadruple helix': toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46*(3/4), 201–234.

Carayannis, E. G., & Campbell, D. F. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69.

Card, N. A. (2012). *Applied meta-analysis for social science research*. New York: Guilford Publications.

Chaitin, G. J. (2009). Evolution of mutating software. *EATCS Bulletin, 97*, 157–164.

Dusa, A., Nelle, D., Stock, G., & Wagner, G. G. (Eds.). (2014). *Facing the future: European research infrastructures for the humanities and social sciences*. Berlin: Scivero.

ESFRI. (2006). European roadmap for research infrastructures. In *Report 2006*. Luxembourg: European Commission.

ESFRI. (2008). European roadmap for research infrastructures. In *Roadmap 2008*. Luxembourg: European Commission.

ESFRI. (2011). Strategy report on research infrastructures. In *Roadmap 2010*. Luxembourg: European Commission.

Etzkowitz, H. (2003). Innovation in innovation: the triple helix of university-industry-government relations. *Social Science Information, 42*, 293–337.

Etzkowitz, H., & Leydesdorff, L. (2003). The dynamics of innovation: From national systems and 'Mode 2' to a triple helix of university–industry–government relations. *Research Policy, 29*, 109–123.

Etzkowitz, H., & Leydesdorff, L. (1998). The endless transition: a triple helix of university-industry-government relations. *Minerva, 36*, 271–288.

Fals Borda, O. (1978). Über das Problem, wie man die Realität erforscht, um sie zu verändern. In H. Moser & H. Ornauer (Eds.), *Internationale Aspekte der Aktionsforschung* (pp. 78–112). München: Kösel.

Foerster, H. V. (Ed.). (1974). *Cybernetics of cybernetics or the control of control and the communication of communication*. Urbana: The Biological Computer Laboratory.

Foerster, H. V. (2003). *Understanding understanding: essays on cybernetics and cognition*. New York: Springer.
Foerster, H. V. (Ed.). (2014). *The beginning of heaven and earth has no name. Seven days with second-order cybernetics*. New York: Fordham University Press.
Funtowicz, S. O., & Ravetz, J. R. (1993). The emergence of post-normal science. In R. V. Schomberg (Ed.), *Science, politics, and morality: scientific uncertainty and decision making* (pp. 85–123). Dordrecht: Kluwer.
Funtowicz, S. O., & Ravetz, J. R. (2001). Post-normal science: Science and governance under conditions of complexity. In M. Decker (Ed.), *Interdisciplinarity in technology assessment: Implementation and its chances and limits* (pp. 15–24). Berlin: Springer.
Gerbode, F. A. (2013). *Beyond psychology: An introduction to metapsychology.* Ann Arbor: Applied Metapsychology International Press.
Gerovitch, S. (2002). *From newspeak to cyberspeak. A history of soviet cybernetics*. Cambridge: The MIT Press.
Gibbons, M., Limoges, C., Nowotny, H., Schwartzman, S., Scott, P., & Trow, M. (1994). *The new production of knowledge: The dynamics of science and research in contemporary societies*. London: Sage Publications.
Glanville, R. (2009). *The black b∞x*, *39 steps* (Vol. III). Wien: Edition Echoraum.
Glanville, R. (2012). *The black b∞x*, *Cybernetic circles* (Vol. I). Wien: Edition Echoraum.
Glanville, R. (2014). *The black b∞x*, *Living in cybernetic circles* (Vol. II). Wien: Edition Echoraum.
Glasersfeld, E. V. (1981). The concepts of adaptation and viability in a radical constructivist theory of knowledge. In I. E. Sigel, D. M. Brodzinsky, & R. M. Golinkoff (Eds.), *Piagetian Theory and Research* (pp. 87–95). Hillsdale: Erlbaum.
Glass, G. V. (1976). Primary, secondary and meta-analysis of research. *Educational Researcher, 5*, 3–8.
Glass, G. V., McGraw, B., & Smith, M. L. (1981). *Meta-analysis in social research*. Beverly Hills: Sage Publications.
Greenwood, D. J., & Levin, M. (2007). *Introduction to action research* (2nd ed.). Thousand Oaks: Sage Publications.
Hayek, F. v. (1967). The theory of complex phenomena. In *Studies in philosophy, politics and economics* (pp. 22–42). London: Routledge & Kegan Paul.
Hayek, F. v. (1972). *Die theorie komplexer phänomene*. Tübingen: J.C.B. Mohr (Paul Siebeck).
Hedges, L. V., & Olkin, I. (1985). *Statistical methods for meta-analysis*. New York: Academic.
Heims, S. J. (1985). *John von Neumann and Norbert wiener. From mathematics to the Technologies of Life and Death*. New York: McGraw Hill.
Heims, S. (1991). *The cybernetics group*. Cambridge: The MIT Press.
Helbing, D. (1993). *Stochastische methoden, nichtlineare dynamik und quantitative modelle sozialer prozesse*. Aachen: Shaker.
Hollingsworth, J. R., & Müller, K. H. (2008). Transforming socio-economics with a new epistemology. *Socio-Economic Review, 6*, 395–426.
Hollingsworth, R. J., & Hollingsworth, E. J. (2011). *Major discoveries, creativity, and the dynamics of science*. Wien: edition echoraum.
Hunt, M. (1999). *How science takes stock: The story of meta-analysis*. New York: Russell Sage.
Hunter, J. E., & Schmidt, F. L. (1990). *Methods of meta-analysis: Correcting error and bias in research findings* (1st ed.). Newbury Park: Sage Publications.
Kahn, H., & Wiener, A. (1967). *The year 2000: A framework for speculation on the next thirty-three years*. New York: MacMillan.
Kajfež-Bogataj, L., Müller, K. H., Svetlik, I., & Toš, N. (Eds.). (2010). *Modern RISC-societies. Towards a new paradigm for societal evolution*. Wien: edition echoraum.
Kauffman, L. H. (1987). Self-reference and recursive forms. *Journal of Social and Biological Structures, 10*, 53–72.
Kauffman, L. H. (2005). Eigen-forms: "Heinz von Foerster in memoriam" [Special issue]. *Kybernetes, 34*(1–2), 129–150.
Kauffman, L. H. (2009). Reflexivity and eigenform: The shape of process. *Constructivist Foundations, 4*(3), 121–137.

Kauffman, L. H. (2017). Cybernetics, reflexivity and second-order science. *Constructivist Foundations*, *3*, 489–497.
Kleiner, B., Renschler, I., Wernli, B., Farago, P., & Joye, D. (Eds.). (2013). *Understanding research infrastructures in the social sciences*. Zürich: Seismo.
Kline, R. R. (2015). *The cybernetics moment or why we call our age the information age*. Baltimore: The Johns Hopkins University Press.
Leydesdorff, L. (2006). *The knowledge-based economy: Modeled, measured, simulated*. Boca Raton: Universal Publishers.
Light, J. S. (2003). *From warfare to welfare. Defense intellectuals and urban problems in cold war America*. Baltimore: The Johns Hopkins University Press.
Malnar, B., & Müller, K. H. (2015). *Surveys and reflexivity. A second-order analysis of the European Social Survey (ESS)*. Wien: edition echoraum.
Mead, M. (1968). Cybernetics of cybernetics. In H. von Foerster et al. (Eds.), *Purposive systems* (pp. 1–11). New York: Spartan Books.
Michael, D. M. (1962). *Cybernation: The silent conquest*. Santa Barbara: Center for the Study of Democratic Institutions.
Müller, A., & Müller, K. H. (Eds.). (2007). *An unfinished revolution? Heinz von Foerster and the Biological Computer Laboratory – BCL, 1958–1976*. Wien: edition echoraum.
Müller, K. H. (2012). *The new science of cybernetics. The evolution of living research designs*. Wien: edition echoraum.
Müller, K. H. (2013a). Lebenslagen, Ungleichheit und Lebensqualität aus radikal konstruktivistischer Perspektive. In F. Kolland & K. H. Müller (Eds.), *Alter und Gesellschaft im Umbruch. Festschrift für Anton Amann* (pp. 219–261). Wien: edition echoraum.
Müller, K. H. (2013b). Second-Order Analysen als neues Aufgabenfeld von sozialwissenschaftlichen Datenarchiven. *e-WISDOM, 6*, 85–106.
Müller, K. H. (2013c). Non-linear innovations. In E. G. Carayannis (Ed.), *Encyclopedia of creativity, invention, innovation, and entrepreneurship* (pp. 1381–1391). Berlin: Springer.
Müller, K. H. (2014). Towards a general methodology for second-order science. *Systemics, Cybernetics and Informatics, 12*(5), 33–42.
Müller, K. H. (2016). *Second-order science. The revolution of scientific structures*. Wien: edition echoraum.
Müller, K. H., & Riegler, A. (2014). Second-order science: A vast and largely unexplored science frontier. *Constructivist Foundations, 10*(1), 7–15.
Müller, K. H., & Toš, N. (2012). *Towards a new kind of social science. Social research in the context of science II and RISC-societies*. Wien: edition echoraum.
Nentwich, M., & König, R. (2012). *Cyberscience 2.0. Research in the age of digital social networks*. Frankfurt: Campus Verlag.
Newman, M. (2005). Power laws, pareto distributions and Zipf's law. *Contemporary Physics, 46*, 323–351.
Newman, M., Barabasi, A. L., & Watts, D. (Eds.). (2006). *The structure and dynamics of networks*. Princeton: Princeton University Press.
Nielsen, M. (2011). *Reinventing discovery. The new era of networked science*. Princeton: Princeton University Press.
Noffke, S., & Somekh, B. (2009). *The SAGE handbook of educational action research*. London: Sage.
Nordman, A., Radder, H., & Schiemann, G. (2011). *Science transformed? Debating claims of an epochal break*. Pittsburgh: University of Pittsburgh Press.
Nowotny, H., Scott, P., & Gibbons, M. (2001). *Re-thinking science. Knowledge and the public in an age of uncertainty*. Cambridge: Polity Press.
Pask, G. (1996). Heinz von Foerster's self-organisation, the progenitor of conversation and interaction theories. *Systems Research, 13*(3), 349–362.
Reason, P., & Bradbury, H. (2001). *The SAGE handbook of action research. Participative inquiry and practice*. London: Sage.

Riegler, A., & Müller, K. H. (Eds.). (2014). Second-order science. *Constructivist Foundations, 10* (1), 7–15. (Special issue).
Rössler, O. E. (1992). *Endophysics. Die Welt des inneren Beobachters*. Berlin: Merwe Verlag. (mit einem Vorwort von Peter Weibel).
Scott, B. (2011). *Explorations in second-order cybernetics. Reflections on cybernetics, psychology and education*. Wien: edition echoraum.
Shneiderman, B. (2008). Science 2.0. *Science, 319*, 1349–1350.
Sornette, D. (2006). *Critical phenomena in natural sciences: Chaos, fractals, selforganization and disorder: Concepts and tools*. Berlin: Springer.
Spencer-Brown, G. (1969). *Laws of form*. London: Allen & Unwin.
Umpleby, S. A. (1991). *Strategies for winning acceptance of second order cybernetics*. Keynote address at the International Symposium on Systems Research, Informatics, and Cybernetics, Baden-Baden.
Umpleby, S. A. (2007). Reflexivity in social systems: The theories of George Soros. *Systems Research and Behavioral Science, 24*, 515–522.
Umpleby, S. A. (2010a). From complexity to reflexivity: Underlying logics used in science. *Journal of the Washington Academy of Sciences, 1*, 15–26.
Umpleby, S. A. (2010b). From complexity to reflexivity: The next step in the systems sciences. In R. Trappl (Ed.), *Cybernetics and systems 2010* (pp. 281–286). Vienna: Austrian Society for Cybernetic Studies.
Umpleby, S. A. (2015). *A global strategy for human development as an example of an alternative goal set in science*. Lecture at the International Society for Systems Science (ISSS), Berlin.
Umpleby, S. A. (2016), Second-order cybernetics as a fundamental revolution in science. Constructivist Foundations, *3*, 455–465.
Van de Vijver, G. (Ed.). (1992). *New perspectives on cybernetics: Self-organization, autonomy and connectionism*. Dordercht: Kluwer.
Waldorp, M. M. (2008). Science 2.0: Great new tool, or great risk? *Scientific American, 298*, 68–73.
Wagner, M., & Weiß, B. (2014). Meta-analyse. In N. Baur & J. Blasius (Eds.), *Handbuch methoden der empirischen sozialforschung* (pp. 1117–1128). Wiesbaden: Springer VS.
Welton, N. J., Sutton, A. J., Cooper, N. J., Abrams, K. R., & Ades, A. E. (2012). *Evidence synthesis for decision making in healthcare*. Chichester: Wiley.
Wheeler, J. A. (1990). Information, physics, quantum: The search for links. In W. Zurek (Ed.), *Complexity, entropy, and the physics of information* (pp. 309–336). Redwood City: Addison-Wesley.
Whitehead, A. (2002). *Meta-analysis of controlled trials*. Chichester: Wiley.
Wiener, N. (1948). *Cybernetics, or control and communication in the animal and the machine*. Cambridge: The MIT Press.

Cyber-Democracy in the Middle East

31

Robert F. Xavier and David F. J. Campbell

Contents

R. F. Xavier (✉)
Middle East Analyst, ThePoliticalMinds.com, Laguna Hills, CA, USA
e-mail: rfrxavier@gmail.com

D. F. J. Campbell
Department for Continuing Education Research and Educational Management, Centre for Educational Management and Higher Education Development, Danube University Krems, Krems, Austria

University of Applied Arts Vienna, Unit for Quality Enhancement (UQE), Vienna, Austria

Faculty for Interdisciplinary Studies (iff), Institute of Science Communication and Higher Education Research (WIHO), Alpen-Adria-University Klagenfurt, Vienna, Austria

Department of Political Science, University of Vienna, Vienna, Austria
e-mail: david.campbell@uni-ak.ac.at; david.campbell@aau.at; david.campbell@univie.ac.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_5

Abstract

As the post development of the Arab Spring unfolds in the Middle East, observers question the effectiveness of Cyber-Democracy in the region. Although regimes have changed, new conflict zones have emerged and are dramatically effecting public opinion on the matter of Democracy. The framework of this discussion will analyze where the direction of the region is headed and to ascertain where the Arab Street stands in the context of the times. Despite positive developments in the use of platforms for Cyber-Democracy, the region is once again at the crossroads presenting conflicting results. The spectrum of measuring success is incredibly diverse and continues to defy what the road to liberal democracy will look like in the Middle East. This analysis aims to answer the question: Is Cyber-Democracy showing progress or regression in the context of the Post-Arab Spring? In addition to answering this question, Egypt and Tunisia will serve as models for failure and limited success, respectively. This analysis will also showcase new polling data shedding light on developing opinions in the region. Finally, challenges of illiberalism in the context of an "Arab Democracy" will be analyzed.

Keywords

Arab Spring · Cyber-Democracy · Democracy · Social media in the Middle East · Muslim Brotherhood · Ennahda · Islamist · Islamism · Salafi · Illiberalism · Arab Youth · The Arab Street · Egypt · Tunisia television media · Quality of democracy

Introduction

The advent of the Arab Spring in the Middle East created dramatic changes to the face of the region. The results of these revolutionary movements yielded great pain towards regression. The region is arguably in one of the most turbulent times in its modern history. It is fitting that experts in this field express we are living in the era of the Post-Arab Spring. Although there is an increase in the usage of the internet and an expansion of connectivity to Cyber-Democracy platforms, authoritarian regimes, media players, foreign powers, and private individuals continue to repress the flourishing of these platforms to discourage progress.

Many shared a genuine hope for change in the Middle East, but this sentiment has now dissipated. At the onset of the Arab Spring experts saw with great anticipation the pinnacle of a 15-year process that showcased the revolutionary dimension of Cyber-Democracy in the Middle East. What sparked the call to action for the Arab Spring was the self-immolation of a Tunisian vegetable vendor named Mohamed Bouazizi in December 2010. Bouazizi's story immediately became publicized throughout the region through social media and more importantly on television. As images and live video became viral showing crowds taking to the streets in Tunisia to protest and topple the Zine El Abidine Ben Ali regime in January 2011, Arab public opinion, or The Arab Street, began to believe that change was possible.

As events unfolded, change appeared to sweep in some of the most solid authoritative Arab regimes. The Arab Street had enough of socioeconomic disparity,

lack of participation in government, and nepotism in the political and economic sphere. As a result, Hosni Mubarak fell in Egypt, Libya's Muammar Gaddafi was assassinated in the streets, and a civil war began in Bashar Al-Assad's Syria. Unfortunately for the states mentioned, all have become volatile. Since 2011, Egypt's Muslim Brotherhood was toppled by a military coup in July 2013 leaving a similar autocratic government in place with Abdel Fattah el-Sisi as president. In Libya, civil war persists and the country continues to exist as a failed state. Syria continues to see horrific strife in an ongoing civil war which has left tremendous collateral damage, a massive refugee crisis, and an open playing field for competing regional and international powers. The impact of the Arab Spring was so severe on Syria that it opened the door for the merger of two militant extremist Islamic groups: the al-Nusra front in Syria with the neighboring Iraqi militant group, The Islamic State of Iraq. These two groups formed the Islamic State in Iraq and Syria or commonly known as ISIS. Combined, ISIS committed itself to fighting the Assad Regime and spreading its influence across the region. ISIS has taken its fight beyond the borders of its "caliphate." In November 2015 the group launched a coordinated terrorist attack in Paris and bombings in Beirut.

The Arab Street continues to observe events unfolding in the Post-Arab Spring leaving them to question the sustainability of democracy in the region. Recent public opinion polling, notably by the ASDA'A Burson-Marsteller and Northwestern University in Qatar, is showing The Arab Street to be considerably unsure about the future prospects of the stability and reliability of democracy in their respective contexts. Although these surveys show that there is healthy growth in internet usage and social media platforms, the prospects of facilitating increased Cyber-Democracy is still in question. They also show the same issues that promoted the Arab Spring are once again at the forefront. The difference today is that the opponents of democratic change are better positioned to stunt the growth of the possibility for revolution.

This analysis aims to answer the question: Is Cyber-Democracy showing progress or regression in the context of the Post-Arab Spring? As it stands, the reality of the situation in the Middle East is that the development of Cyber-Democracy still continues to grow, but the results of the Arab Spring overwhelming led to regression. In order to present this conclusion, the intention here is to uncover the reasons for regression; analyze two case studies, Egypt and Tunisia; showcase the dynamics of The Arab Street as discovered in recent polls; and to finally discuss the concept of illiberalism in the context of an Arab Democracy. To conclude, this chapter will look at future challenges and potential prospects for Cyber-Democracy in the Middle East.

Regression Post-Arab Spring

State Reactions After the Arab Spring

The outcome of the Post-Arab Spring created a different reality for Cyber-Democracy platforms. Its effects offer a double-edged sword for an uptrend of democracy in the region. On the one hand, the accessibility of these platforms is available, but governments in the region are mobilizing to counterrevolutionary

trends. Moroccan physician and blogger, Hisham al-Miraat, explains to the Committee to Protect Journalists (CPJ) that:

> The Arab Spring has had two consequences. . .It showed that you can change things in your country, but it was also a wake-up call to those governments – it was a paradigm shift in the online world. Before, those governments thought the Internet could not undermine the structures they had spent centuries building. But the Internet is ubiquitous; you can't just shut it down. (Radsch 2015)

Al-Miraat's conclusions are justified because many governments in the region made internet accessibility a top priority through internal technology development programs when the internet first emerged. Unfortunately, the consequences of the revolutions enabled governments in the region to move against Cyber-Democracy platforms (Xavier and Campbell 2014, pp. 155–156).

In Egypt, the Mubarak government made information and communications technology (ICT) a strategic priority since 1999 (Freedom House 2015, p. 270). From 1993 to 2008, internet control was relaxed, but as online campaigns exposed government repression, the state police during 2008–2011 conducted surveillance, censorship, and cyberattacks against opposition groups – particularly the Muslim Brotherhood (Freedom House 2014, p. 260). Even after the Arab Spring, restrictions and surveillance continues to be a major factor in hindering free speech in Egypt. Although a new constitution guarantying freedom of speech was passed in a referendum in 2014, concerns are still present over vague provisions allowing the government to censor free speech in certain cases. In addition, telecommunications services have repeatedly been suspended in the Sinai Peninsula where military operations take place (Freedom House 2014, p. 259). In August 2015, an anti-terrorism law was enacted and has created fears that provisions within the law can be used against online activists and critics of the government. A cybercrime law is also in the works of being ratified by the president which criminalizes a broad spectrum of potential online offenses. Lastly, journalists and online activists continue to face imprisonment or are serving sentences for allegedly opposing the state (Freedom House 2015, p. 268).

Tunisia's story is different from Egypt in relation to the internet's introduction to the Post-Arab Spring. The internet was publically launched in Tunisia in 1996 and broadband was made available in 2003. The internet landscape during the Ben Ali era was extensively restricted despite having built a relatively advanced infrastructure and a developed telecommunications market. The restriction efforts of the regime developed Tunisia's online reputation as being an "internet enemy." Despite its reputation, Tunisia made great strides in creating a freer internet. Few cases of online restrictions have been documented in Tunisia following the revolution, although the judiciary continues to impede in this area. In 2012 Tunisia joined a coalition of governments focused on advancing internet freedom and hosted the third Freedom Online Conference in 2013. Finally, with the passing of the new constitution in 2014, protection of free speech is guaranteed and prior censorship is banned, but there are still several laws from the Ben Ali era that continue to test the validity of the freedoms offered in the constitution (Freedom House 2014, p. 783).

Throughout the region, several governments have enacted legislation limiting the ability for independent journalist or freedom activists to utilize the internet. Many states have enacted cybercrime laws to counter the use of the internet through the justification of protecting the state against terrorism. As a result, according to the CPJ, over 30 online journalists were arrested in the Arab Middle East in 2014 under vague provisions of cybercrime and antiterrorism laws. In the case of the United Arab Emirates (UAE), the cybercrime law was updated to "make it illegal to defame the government or injure its representation" (Radsch 2015). Monitoring and surveillance measures have been established in Jordan and Saudi Arabia. Under these laws, news websites and blogs must register with the state. Similar laws are in place in other Gulf Arab countries like Kuwait and Qatar. In Kuwait, a law has been proposed to allow authorities to block or shut down the internet without reason. Qatar passed a cybercrime law in September 2014 which grants the government authority to impose fines and prison sentences for publishing content that violate social values (Radsch 2015).

It is evident that states in the region are aware of the effectiveness of Cyber-Democracy platforms. There are more examples proving that governments in the region are taking more provocative steps to thwart the threat of Cyber-Democracy platforms. In most cases in the region, governments have used the excuse of countering terror threats in order to have more control over the internet. Despite these challenges, later sections in this discussion will show that restrictions on the internet are not necessarily unpopular with The Arab Street. Even though these measures have been enacted, the use of the internet continues to be a very important force in the region.

What Went Wrong with Cyber-Democracy After the Arab Spring?

The Arab Spring showcased the revolutionary dimension of Cyber-Democracy in a manner appearing to encourage democratization in a region heavily entrenched in autocracy. Cyber-Democracy platforms like Facebook, Twitter, and media helped encourage a captive audience to believe that change was possible. The role Cyber-Democracy played during this time cannot be underestimated, but deeper analysis into the Arab Spring shows economic grievances created the basis for these revolutionary movements. As a result, media outlets like Al-Jazeera were at the forefront in broadcasting these events to the Arab Street. As public displays of protest were broadcasted region-wide, the Arab Street figured that if the self-immolation of a vegetable vendor could change the face of a nation in Tunisia then onlookers in other countries like Egypt could do the same (Xavier and Campbell 2014, pp. 157–161).

Arab media expert Marc Lynch implies media played a significant role in creating the trend toward regression for democratic transition in the Middle East (see Xavier and Campbell 2014, pp. 167–168). Lynch claims media organizations who proved to be catalyst for the revolutions in the region rapidly degenerated into serving the agendas of state authorities or political factions to counter democratic change. Consequently, the media "played a destructive role during the attempted transitions for three major reasons: political capture, the marketing of fear, and polarization" (Lynch 2015, p. 91). This claim is reinforced with Al-Jazeera specifically, seeing the station began supporting the

interests of its state patron, Qatar. The Egyptian government also followed suit with this interpretation claiming that Al-Jazeera broadcasted with bias in favor of the Muslim Brotherhood. The Egyptian Interior Ministry raided the station's offices in Cairo in December 2013 and arrested several journalists on charges of spreading "rumors and false news" (El Deeb 2013). Although several activists were released in September 2015 including two key Al-Jazeera journalists, several are still incarcerated (Al-Jazeera 2015). Furthermore, as Lynch points out, "Al Jazeera came to be identified with Egypt's Muslim Brotherhood and Tunisia's Ennahda, while other stations peddled wild, sensational stories that fed anti-Islamist anger and suspicion" (Lynch 2015, p. 93).

Broadcast media or television is still an important factor in the evolution of Cyber-Democracy in the Middle East. In relation to online activism in the region, if it were not for the launch of Qatari-based Al-Jazeera in 1996, Cyber-Democracy platforms may have developed at a slower pace (Xavier and Campbell 2014, pp. 151–153). The importance of Al-Jazeera is critical, for it offered its audience a narrative of the region's current events without state-run bias. Prior to its inception, media in the region was primarily offered through the prism of the state's agenda (Salvatore 2013, pp. 6–7).

As it relates to state media, Lynch explains that this sector continues to resist reform and serves the interest of the state or elite patrons. For broadcast media, new television stations emerging on the media scene tailor their content according to the political interests of their patrons. Limited reform emerged in Morocco and Jordan, but these reforms yielded the marketing of constitutional reforms while adding to fears of horrific unrest. In Libya and Yemen, both failed states, local media also portrayed the bias of political factions which created further "polarization, fear, and insecurity" (Lynch 2015, p. 96). The national media sphere effectively spiraled backwards to their prerevolutionary positions, detracting democratic evolution. As Lynch concludes, the state media maintained the traditional "rules of the game" leaving broadcast media and print media "in the hands of elites who had benefited from the old order and so feared change" (Lynch 2015, pp. 93–94).

Social media, a Cyber-Democracy platform, is another factor contributing to the regression of the revolutionary ambitions of the Arab Spring. Regression in this area continues to fester polarization and even isolation of political groups. Sadly, social media also served to enhance fear of democratization. Lynch adds that although social media is important, he makes the distinction that social media worked in tandem with broadcast media, thereby "forming a singular media ecology: Broadcast-media content circulated frequently via social media" (Lynch 2015, p. 92). Despite the Western focus on social media platforms during the Arab Spring, television still serves as the primary source of information for the Arab Street. Lynch states social media can create the call for activism, but it may not lead to democratization. It has helped isolate individuals into "informational clusters" where one's ideology or political leaning is reinforced. Although these clusters are challenged by opposing clusters from time to time, they also create a false sense of unity in one's respective political-ideological camp. In the context of the "social media Arab Street," the extremist camp has benefited from this (Lynch 2015, p. 97). Finally, Lynch concludes that these realities "amplified extreme voices, gave wing to baleful rumors, and kept the center from holding" (Lynch 2015, p. 96).

Table 1 Internet and Facebook usage/penetration in the Middle East, Egypt, and Tunisia

	Middle East	Egypt	Tunisia
Internet usage			
2012	90,000,000	29,800,000	4,100,000
2015	123,172,132	48,300,000	5,408,240
Net gain	33,173,132	18,500,000	1,308,240
Facebook usage			
2012	28,800,000	12,100,000	3,300,000
2015	49,400,000	27,000,000	5,200,000
Net gain	20,600,000	14,900,000	1,900,000
Internet penetration of population			
2012	40.2%	35.6%	39.1%
2015	52.2%	54.6%	49.0%
Net gain	12.0%	19.0%	9.9%
Facebook penetration of internet users			
2012	32.0%	40.6%	80.4%
2015	39.7%	55.9%	96.1%
Net gain	7.7%	15.3%	15.7%

Source: Data for 2012: Xavier and Campbell, pp. 149–150
Data for 2015: Internet World Stats 2015

The dichotomy of the Post-Arab Spring presented in this section is heavily focused on the dimension of Cyber-Democracy. Several other factors also contributed to the regression of the Arab Spring whether it be international responses, direct intervention by regional players, or involvement of Western powers. As Lynch's argument relates to Cyber-Democracy, regression stems from platforms initially used during the Arab Spring and subsequently reversing the tide for change by conflicting agendas of elites and nonelite individuals. This calls to mind the dual nature of Cyber-Democracy impacting many who were more inclined to use these platforms for democratization. As polling data will show in the following section, the idea of nurturing Cyber-Democracy with the use of media or web-based platforms is struggling to capture the hearts and minds of the Arab Street (see Table 1).

Surveys of the Arab Street

Understanding the perception of the Arab Street on Cyber-Democracy has produced unique findings on where the region is headed in the areas of the usage of platforms and how they are shaping opinions on the effectiveness towards democratization. This section will highlight two studies: (1) "Media Use in the Middle East: An Eight-Nation Survey by Northwestern University in Qatar (2013)" and (2) the "7th Annual Arab Youth Survey 2015" by ASDA'A Burson-Marsteller. Northwestern's study focuses on data collected on media use (internet, television, and face-to-face interaction) in three geographic sectors of the Arab world: The Levant, North Africa, and

the Gulf States. Within these sectors, the study focused on the following nations: Bahrain, Egypt, Jordan, Saudi Arabia, Lebanon, Qatar, Tunisia, and the United Arab Emirates. The study conducted 10,000 interviews, 90% face-to-face, in most of these countries. The ASDA'A Burson-Masteller Arab Youth Survey 2015 presents insight into "the concerns and aspirations of Arab youth, their views on the economy and the impact of the Arab Spring, their media consumption habits, and attitudes towards traditional values and the people who influence them" (p. 4). The survey conducted 3500 face-to-face interviews with Arab men and women ages 18–24 from January 20 to February 12, 2015, in 16 Arab countries. The countries surveyed were: Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, the United Arab Emirates, Algeria, Egypt, Iraq, Jordan, Lebanon, Libya, Morocco, Palestine, Tunisia, and Yemen.

Media Use in the Middle East

Media use and perception in the Middle East is an area of study offering interesting results. The 2013 study conducted by Northwestern University in Qatar supported this conclusion by noting survey data offered paradoxes on media perception in the Middle East. On the one hand, media use continues to grow in the region, but attitudes on this subject are conflicting. Generally speaking, there is optimism in most countries on media credibility and quality, but in countries like Egypt, Lebanon, and Tunisia, media credibility shows less favor (Dennis et al. 2013, p. 8). The study maintains that the most important platform for media is television with Al-Jazeera being the top source for news in the region. An overwhelming majority of adults (98%) in the Middle East watch television (Dennis et al. 2013, p. 15). The survey highlights the importance of interpersonal interactions when it comes to obtaining information in the Middle East, and it is a point in this discussion that deserves proper attention. To briefly summarize, the survey states:

> While commentators in the west decry the intrusion of the internet on interpersonal communication and the death of conversation, this is assuredly not the case in the Arab world, where interpersonal communication continues to play a powerful role–even in online communication (social communication online is the most popular activity reported by those in the survey). (Dennis et al. 2013, p. 95)

The internet is the second most used media platform in the Middle East. The internet is used roughly 3 h a day in the home and is heavily used in the Gulf Arab States. Online usage has developed a generation gap where "82% of people under the age of 25 use the internet, compared to only 37% of those over 45" (Dennis et al. 2013, p. 11). In total, over 66% of all adults use the internet. By comparison: 91% of adults use the internet in the UAE, 86% in Qatar, 82% in Bahrain and Saudi Arabia; whereas, 22% of Egyptians and 46% of Jordanians use the internet (Dennis et al. 2013 p. 17). Roughly 75% of online users in the Middle East use wireless devices (smartphones and laptops) to access the internet (Dennis et al. 2013, p. 11). Social networking is widespread with online users in the region. Facebook is the most

popular social media platform, although other platforms are gaining ground. New strides have been made in closing the language gap with online usage, and Arabic has surpassed English on most online media platforms in the region (Dennis et al. 2013, p. 8). Adults on the internet in the Middle East use a variety of different online media sources for new consumption, namely within the Arab language sphere and Western media outlets. In the countries surveyed over 55% use Arab websites for regional news while 35% use Western sources. For news concerning Europe and America, 34% of adults use Arab websites and 29% use Western websites (Dennis et al. 2013, p. 36).

The emphasis on sources for news and current events are spread across different platforms. Television is still the top source for news where 83% of adults access it. Egypt, Jordan, Saudi Arabia, and Lebanon are the most reliant on television for news and current events. Interpersonal sources, namely family and friends, are second where 72% of adults rely on this source for information. Over 65% of adults see the internet as an important source for news which surpasses newspapers at 53% and radio at 47%. In Qatar, 70% of adults use internet sources for news and find it more important than television (58%). This is a striking trend seeing that Al-Jazeera, a Qatari news broadcaster, is the most important source for news in the region. Age demographics show that television is prominent with all age groups, but print media and radio show a divergence. The older generation is more likely to use these platforms for information while the younger generation (74% under the age of 25) gravitates towards digital media for information (Dennis et al. 2013, pp. 24–25). News consumption is utilized both at the local and international levels. Although local news is the most sought after by 73% of adults, regional (53%) and international (43%) are equally important and are also followed. The Gulf States tend to follow regional and international news respectively; Egyptians and Tunisians are far more interested in national news over regional or international news (Dennis et al. 2013, p. 34).

Understanding the effectiveness of online political development is lagging with people surveyed in the Middle East. Generally speaking, the internet is viewed as an effective tool for political development, yet in the Middle East, this sentiment is being tested. On cosmetic subjects such as technology, life issues, and consumer goods, the public views that the internet is very effective in influencing opinions. On the political front, 49% of adults find that the internet will enable them to have more say in their government. Within that sample, 48% believe that the internet will provide them with more political influence on their government. Despite this, most people believe that the internet does provide for better understanding of politics. Polling in Saudi Arabia displays more optimistic opinions on the effectiveness of the internet on politics. Over 71% of Saudis believe that the internet provides for a better understanding of politics. In addition, 63% of Saudis feel that the internet will give the public more influence on politics (Dennis et al. 2013, pp. 59–60).

Opinions on regulation of the internet offers paradoxes highlighted in the study. As it relates to the freedom of expression on the internet, 61% of adults in the Middle East believe that it is acceptable to voice their opinions online even if they are unpopular. In contrast to this opinion, 50% of adults in the Middle East believe that

there should be more regulation over the internet, yet 51% feel that there is not enough awareness of present regulation on the internet today. The study presents that support for increased regulation on the internet is strong in Saudi Arabia (62%), Lebanon (64%), Qatar (57%), and Tunisia (52%). Confidence in expressing opinions about politics on the internet is low where 47% of adults in the region believe it is safe to express their opinions on the internet. Age disparities also emerge in the survey. Most young people in the Middle East are trusting of the internet than older adults. Half of adults under 25 believe it is safe to voice their opinions online while 41% of adults 45 and older agree. This example also transmits to political advocacy, 48% of young adults are likely to advocate for online political freedom whereas 41% of adults 45 and older are willing to do the same. Finally, 55% of adults under the age of 25 and 45% of adults 45 and older favor increased online regulation in their country (Dennis et al. 2013, pp. 55–56).

The Legacy of the Arab Spring on Arab Youth

The Arab Spring left a tremendous impact on the youth of the Middle East. Presenting the findings of the ASDA'A Burson-Marsteller Arab Youth Survey offers insight into how the youth of the Middle East see the course of Arab Spring unfolding. The sentiment surrounding democratization in the Middle East is summarized with uncertainty from the youth. Overall, the breakdown of the findings concludes that democracy in the region is still facing challenges. The youth in the Middle East are cautiously optimistic about future prospects in their respective countries. The UAE continues to be the favored model for emulation for the fourth year in a row. Lastly, on the media front, although digital media is making ground, youth in the Middle East prefer to seek information on current events from television (ASDA'A Burson-Marsteller 2015, pp. 6–7).

When asked if the Middle East is better off after the Arab Spring, youth in the Middle East responded with uncertainty almost rejecting the notion that democracy could work in the region. Confidence in the outcome of the Arab Spring has been declining since 2012. Polling showed that in 2012, 72% of youth agreed that the Arab World was better off after the Arab Spring. These numbers start to decline in 2013 to 70%, in 2014 to 54%, and again in 2015 to 38%. In regards to being better off in 5 years after the uprisings, 41% felt they would be in 2015, 51% in 2014, 74% in 2013, and 71% in 2012. In response to the statement "democracy will never work in the region," 39% agreed with the statement while 36% disagreed and 25% were not sure. When looking at countries individually negative opinions on democracy working in the region were shared by a majority in Yemen, Qatar, Saudi Arabia, Oman, and Tunisia (46%). On the other hand, Kuwait, Iraq, Libya, UAE, and Palestine were optimistic about democracy working in the region (ASDA'A Burson-Marsteller 2015, p. 8).

The youth is very concerned about the threat of ISIS, and most are not confident that their governments can deal with the group. Over 73% of Arab youth are

concerned with the group's growing influence where 37% believe that it is the region's greatest obstacle. Although collectively 47% believe that their governments cannot deal with the group, confidence is strong in places like Algeria (83%) and to a lesser degree in the Gulf Arab states where 60% of respondents believe their governments can deal with ISIS. Unlike the Gulf States, Lebanon is the leading country in the region that believes (77%) its government cannot deal with the ISIS threat (ASDA'A Burson-Marsteller 2015, p. 10).

Despite security, economic and political concerns, youth in the region are cautiously optimistic about the future. Looking at the three subregions in the Middle East, 83% of Gulf Arab youth, 57% of North Africans, and 29% in the Levant believe that their country is headed in the right direction. In terms of general optimism, 67% in the region believe the future will be better while 26% believe the past was better. Approximately 70% of Gulf and North African respondents believe the future will be better while 57% feel the same way in the Levant (ASDA'A Burson-Marsteller 2015, p. 14).

The United Arab Emirates is the favored place to live among Arab youth. Known as an economic marvel, the UAE leaves a great impact on the Arab youth. Its appeal surpasses western countries like the United States, Germany, and Canada. When presented a list of 20 countries, over 20% want to live in the UAE, 13% in the United States, and 10% in Germany and Canada. On the point of emulation, 22% want to see their country become like the UAE, 15% like the United States, and Germany 11%. The study concludes that the popularity of the UAE is largely due to expected continued economic growth and the perception that the Emirates encourages an environment for young Arabs to achieve one's full potential (ASDA'A Burson-Marsteller 2015, p. 18).

Media use by Arab youth is consistent with most surveys of the region. Digital media continues to grow at a fast rate, but television is still a key source for media consumption. According to the survey "television remains the most popular source of news (60%), 40% of young Arabs get their news from online sources and 25% from social media" (ASDA'A Burson-Marsteller 2015, p. 26). Social media makes strides as a growing platform for information, 91% of respondents visit a social media platform at least once a week. The largest consumer of social media in the Middle East is the Gulf.

The presentation of these surveys reveals the important dynamics of where the Arab Street stands after the Arab Spring. It is clear that the use of Cyber-Democracy platforms is playing a very critical role in accessing information. Social media and the internet are quickly rivaling television, but the power of news broadcasting still champions the media sphere. The surveys show that there are paradoxes in relating Cyber-Democracy platforms to the general favorability of democratization. Several issues may be contributing to this issue. First, the broadcasting of instability in countries where the Arab Spring took place is certainly on the mind of the Arab Street. As indicated, the optimism surrounding the Arab Spring in the initial years following it continues to slide consistently. Second, the Arab Street is also skeptical on the effectiveness of the internet on the political sphere citing that the internet is most reliable in matters of cosmetic subjects. This

is revealed in the striking support for increased regulation on the internet as a whole. At the same time, it can also imply that the internet is more effective than the Arab Street is willing to admit. Noting Lynch's conclusions, the "like-minded" knowledge clusters could be a potential reason for this. Third, it can be implied from the data that the Arab Street is seeking a stable political system over dealing with the challenges of developing democracy in their own countries. This is inferred from the consistent favorability of the young Arab Street wanting to emulate the United Arab Emirates. The UAE is ruled by a monarch, but given its economic success and offering the perception that it enables an individual to achieve his full potential, offers a very compelling argument that the Arab youth searches for these elements in their own societies. Despite these challenges, the use of Cyber-Democracy platforms can still be a vehicle for democratization in the future.

Egypt and Tunisia

Egypt and Tunisia provide a good example of comparison as it relates to the revolutionary movements that took place in their respective contexts. Comparing Egypt and Tunisia offers insight into two separate paths of political development. Overall Tunisia is heralded as a bumpy success story while Egypt is viewed as a democratic failure despite maintaining limited stability. Politically, both countries saw the rise of Islamist parties emerge to power after their revolutions – the Ennahda in Tunisia and the Muslim Brotherhood in Egypt. Both parties were founded by the same political ideology, but the divergence on the orthodoxy of that ideology became apparent in developing their party programs in their respective political systems. Interestingly, Tunisia's Ennahda became suspicious of the Muslim Brotherhood as they carefully watched events unfold in Egypt. The Muslim Brotherhood, on the other hand, maintained its ideological platform to its detriment and was overthrown by a military coup in 2013.

The catalyst for change in both countries was fueled by similar reasons, consequently protests in Tunisia subsequently influenced protests in Egypt. Motivations for change in both countries were driven primarily by economic grievances rather than political ideals. The two countries diverge in respect to the demographics of the protestors. In Egypt, the protestors were mainly from the middle class whereas in Tunisia the protestors were a broad-class coalition. Protestors with middle-class occupations accounted for 55% in Egypt and 30% in Tunisia. Demonstrators representing workers, students, and the unemployed accounted for 19% in Egypt, yet in Tunisia they accounted for 57%. Age demographics were also different; in Egypt they were primarily middle-aged while in Tunisia they were significantly younger. Lastly, civil society associations such as the Muslim Brotherhood played a greater role in Egypt than they did in Tunisia (Beissinger et al. 2015).

Political Progression in Tunisia

The political progression in Tunisia was effected by regional developments which in turn guided internal dynamics for a more inclusive political system. In essence, since the revolution in 2011, Tunisia can be considered a fragile, yet genuine Arab democracy (Marks 2015, p. 1). To expand on this claim one must understand the internal dynamics Tunisia faced in its postrevolutionary context. Although Ennahda emerged from the Muslim Brotherhood's school of Islamism, it never held real power in the Tunisian political sphere before the revolution. The party was banned in the country forcing many of its members to flee aboard. This is a stark contrast from the Egyptian Muslim Brotherhood seeing that it had played a role in the Egyptian political and social sphere for many years prior to the revolution. Ennahda, on the other hand, reentered Tunisian politics as a result of the revolution. From the onset, Ennahda was looked at through the prism of the Muslim Brotherhood, and there was fear the movement would popularize jihadism and promote an Egyptian-style Islamist state (Marks 2015, p. 2).

Monica Marks from the University of Oxford correctly maintains that regional developments such as the rise of ISIS, the Egyptian Military Coup of 2013, and local challenges effected Ennahda's behavior. Marks concludes "the primary effect of these developments forced Ennahda into a defensive posture, narrowing its range of political maneuver" (Marks 2015, p. 1). Having rejoined the political scene and winning a plurality in the 2011 elections, Ennahda was aware of the suspicion it faced from the opposition. In reaction to this, the Islamists created a cross-coalition government with secular parties. In conducting interviews with Ennahda members (Nahdawis), she was amazed to discover a majority of Nahdawis did not view the Egyptian Muslim Brotherhood as the political model they wanted to follow. In contrast, the Nahdawis were more interested in emulating the Turkish Islamist party AK Parti or even the German Christian Democrats. Finally, the idea of creating a theocratic regime like Iran or Saudi Arabia was also viewed as a nonoption.

This sentiment was shared by the Ennahda president, Rached Ghannouchi. In her interview with Ghannouchi, Marks points out that he was careful to avoid mentioning the Muslim Brotherhood, but instead he validated the Turkish model stating the "AK Parti will gradually make Turkey a more Muslim country. . .Through education, building the economy, and diversifying the media. That's our model – not law. Make people love Islam, don't coerce them" (Marks 2015, p. 3). Effectively, as Marks says, the Nahdawis began to view themselves as more enlightened than their Muslim Brotherhood contemporaries. Criticism of the Muslim Brotherhood was prevalent with Nahdawis to the degree of frustration. They felt that events unfolding in Egypt with the Muslim Brotherhood at the helm was impeding on the success of Ennahda in Tunisia. Moreover, Ghannouchi addressed Cairo in October 2013 and warned Egypt's Muslim Brotherhood of enacting a "democracy of the majority," concluding that power must be balanced, and that diverse societies must accept diversity or face chaos (Marks 2015, p. 4).

Ennahda also faced another headwind with extremist Islamist factions within the political sphere. Youth in Tunisia were being influenced by Salafi jihadism, an aggressive and violent form of Islamism, through online content emerging from the Gulf States. Consequently, over 3,000 Tunisians were fighting in Syria for ISIS. The Salafist movement in the view of Ennahda was bewildering. Ennahda leadership viewed this segment as a misguided trend among the youth resulting from marginalization from the eras of Ben Ali and his predecessor Habib Bourguiba. Ennahda argued that weakening the Zaytouna, a historic center of religious learning, during the Ben Ali and Bourguiba eras created a vacuum for extremist Islamism to be propagated among the youth. Ennahda reacted to this trend by reviving the Zaytouna so that they could bring the Salafi youth into the fold of progressive discussion to thwart their views. This created a generation gap between the youth and their parents who were more inclined to follow the gradualist approach of Islamism rather than their Salafi-influenced children (Marks 2015, p. 5).

Support for Ennahda declined after the revolution as terrorism was intensified by Salafi jihadists. Attacks carried out during 2012 and 2013 led Ennahda to declare the largest Salafist Jihadi group, Ansar Al-Sharia, a terrorist organization. In addition to its declaration, Ennahda began revisiting Ben Ali era measures to crackdown on the group. These measures were heavily criticized as being too soft on the Salafists by the opposition leftist party Nidaa Tunis. As a result of the breakdown in the security situation and Ennahda's willingness to include the opposition, the Nidaa Tunis party – a party consisting of "leftists, business elites, and officials from the Bourguiba and Ben Ali Regimes" – won parliamentary and presidential elections in the fall of 2014 (Marks 2015, p. 7).

The victory of Nidaa Tunis was not solely centered on security issues. Ennahda's approach to changing regional dynamics, namely ISIS in Syria and the coup in Egypt, directed the party towards inclusion of the opposition. The Egyptian coup was especially at the forefront during the drafting of the new Tunisian constitution in 2013. Initially, Ennahda attempted lustration against the opposition, but protests in the streets led to a retraction of support for this measure by the party leadership. Fortunately, the constitution was passed and power was temporarily handed to a technocratic caretaker government. This change in rhetoric by Ennahda did not come easily. Rached Ghannouchi is mainly credited for convincing members of his party to accept an abandonment of lustration and open the playing field for other parties. Ghannouchi feared that if his party was not willing to bend, the revolution could be reversed. He stressed that Tunisia was in a period of transitional politics (Marks 2015, pp. 9–10).

The Tunisian case offers an example of a transition in politics which is in line with the needs of its political context. It proves that internal dynamics while being influenced by external dynamics impacted the transition for democracy in Tunisia. The discussion presented on Tunisia offers a key conclusion; it is a model for progression. The leadership of the Ennahda party maintained a progressive approach during the transition, for had they taken the approach of their Muslim Brotherhood cousins in Egypt, progression may have been reversed. Tunisia's democracy is still fragile. Several issues continue to dominate the political scene. Unemployment is

still a factor, and security concerns following the terrorist attacks on the beach resort in Sousse and the Bardo National Museum in 2015 are still in play. Regional issues like the civil war in Syria and increasing terrorist activity of ISIS will also continue to impact extremist factions in Tunisia, yet it may conversely encourage the country to stay the course towards sustained democracy to avoid carnage domestically.

Political Regression in Egypt

The Egyptian case offers a basis for democratic regression in the political system. In comparison to its Ennahda cousins, the Muslim Brotherhood's inability to moderate its ideology or make compromises led to its downfall. The fall of the Mubarak regime in 2011 yielded a 2-year rule of the Muslim Brotherhood in Egypt until it was overthrown in July 2013. The revolution in 2011 left Egypt in an uneasy power arrangement partnering military, security, and political institutions in a "power triangle" (Kandil 2014). This uneasy arrangement left the security apparatus falling behind the military while the political sphere was open to negotiation with the Brotherhood seeking to present itself as the best option for governing to the others. Despite appeasing both sides, the Brotherhood swiftly moved to seize control of the revolution and left little for the other ends of the triangle to participate in developing the state. Consequently, the opposition became solidified and moved against the Brotherhood to regain control (Kandil 2014).

In 2013, Reuters conducted interviews with politicians, youth activists, diplomats, and military officials in Egypt. The news agency uncovered that initially the Muslim Brotherhood was not interested in taking control of the government. It was viewed among Brotherhood members that Egypt was not ready for the Muslim Brotherhood to govern and that one political actor could not rule alone. After the Brotherhood allied with smaller Islamist parties, it gained control of the parliament, and the party quickly realized it still did not have the power to make legislative changes. This left some Brotherhood members frustrated and created the momentum to call for control of the presidency. The sentiment was encouraged by younger members. Despite objection from the Brotherhood's Guidance Office, the young element headed to social media to promote the idea of seeking the presidential nomination. Opposition for the measure was still fierce for the reason of creating suspicion. After intense debate and several rounds of votes, a slim majority of members voted in favor of running a candidate for the presidency (Blair et al. 2013).

The debate over the candidacy was also an uphill battle. The Brotherhood sought two respected pro-Mubarak judges as candidates, but they declined. Khairat El-Shater, the deputy leader of the Brotherhood, was disqualified as a candidate due to his criminal record, and finally the choice was given to Muhammad Morsi. According to interviews by Reuters, Morsi was reluctant in accepting the position. Morsi defeated Ahmed Shafik, a former air force general and final loyal prime minister of Mubarak by a thin majority. Shafik was hated by liberals and leftists, and as a result, they supported Morsi. Their support for Morsi was reinforced by promises of participation in the new government and drafting the new constitution.

Despite these promises, the development of the constitution created clashes with secular parties and civil society groups alike. Dissatisfaction on the points of the constitution were centered on "ambiguous wording on freedom of expression, and the absence of explicit guarantees of the rights of women, Christians and non-government organizations" (Blair et al. 2013). In addition, Morsi circumvented the judiciary by declaring the constitutional assembly was above judicial review along with the president. Seeing that the judiciary was filled by Mubarak appointees, Morsi feared that they would attempt to undo the Brotherhood's political gains. The entire process to develop the constitution also shunned members of Morsi's own party. Ignoring warnings from his own staff, many in the Brotherhood hierarchy concluded that Morsi was far too self-confident in his approach.

From December 2012 to the late spring of 2013 demonstrations in the streets voiced disapproval of the moves made by the Morsi government. In the meantime, the military maintained neutrality as it did during the first revolution. In the early days of the new presidency, Morsi removed top generals in the military to strengthen his influence over the organization. Consequently, the same general that Morsi appointed as commander, General Abdel Fattah al-Sisi, would become the new president of Egypt following the coup in the Summer of 2013. According to the Reuters report, members in the military claimed that Morsi made a critical miscalculation in appointing al-Sisi. The military was happy to see the old-guard retired and allowed it to happened, but they still looked at Morsi with great suspicion. In January 2013 the military warned that unrest in the country would lead to collapse and it maintained itself as the "'solid and cohesive block' on which the state rests" (Blair et al. 2013).

The economic situation in Egypt was also crumbling. The military had effectively left the economy in shambles during its interim rule following the revolution. Energy prices were rising, and the state's efforts to subsidize costs in the domestic sphere were becoming limited. Moreover, regional financial support from Saudi Arabia and the United Arab Emirates was significantly reduced due to Brotherhood opposition to the Gulf Monarchies. Qatar and Turkey were still offering support to the Morsi government, but this was not enough. Loans from the International Monetary Fund (IMF) were also considered, but this was rejected by the military during its interim rule. The military feared that taking a loan from the IMF would spark more protests. Finally, chances of getting a loan diminished after Morsi issued the constitutional decree. Time had run out for the Muslim Brotherhood. They began blaming pro-Mubarak elements in the country for inciting economic strife, but these accusations fell on deaf ears leading Egyptians to blame the Brotherhood government. As protests raged on, the military took decisive action in overthrowing the Muslim Brotherhood.

Interestingly, there were attempts by factions in Egypt to avoid a disintegration of the government prior to the military coup. Reuters uncovered through its interviews that efforts were made in the final days of the Muslim Brotherhood regime to salvage the situation. In the month leading to the coup, two chief power brokers, Amr Moussa, a former Mubarak era foreign minister and secular nationalist politician, and Khairat El-Shater met at the home of liberal politician Ayman Nour to

avoid collapse (Blair et al. 2013). According to Moussa, El-Shater claimed the "government's problems were due to the 'non-cooperation of the 'deep state' – the entrenched interests in the army, the security services, some of the judiciary and the bureaucracy" (Blair et al. 2013). Moussa concluded after his meeting with El-Shater that the Muslim Brotherhood was not willing to change and that they were "over-confident, incompetent in government and had poor intelligence on what was brewing in the streets and the barracks" (Blair et al. 2013). After the overthrow of Morsi, a court in Egypt in the summer of 2014 dissolved the political wing of the Muslim Brotherhood from participating in parliamentary elections, only allowing Brotherhood candidates to run independently or form a new party. The government also designated the group as a terrorist organization after allegations that the group incited violence and had links to jihadists in the Sinai Peninsula. In addition, the new constitution does not allow political parties to be formed on a religious basis (BBC, August 9, 2014).

Identifying these case studies offers insight into the initial developments of Arab democracy in Egypt and Tunisia. The key difference that separates these two cases is the manner in which political elites reacted to the changing political environment. For the Tunisian Ennahda, accepting the risk of making compromises and allowing for competition among political parties aided in maintaining the goals of the revolution. Repression of plurality in the political sphere could not be accepted because it would reject the efforts of the revolution itself. In Egypt, the Muslim Brotherhood believed its power was consolidated. With this in mind, the Brotherhood was not willing to accept that they mismanaged the political and economic situation in Egypt. As presented, the opposition was even willing to provide olive branches to the Brotherhood in order to hold the country together, but the Brotherhood would not accept this as option. The end result was a military coup. The military and opposition factions determined that the stability of Egypt was more critical than seeing the Muslim Brotherhood lead the country to total collapse. To conclude, both cases present value in serving as a model for future development of democratic systems in Arab countries.

Testing Liberalism in the Middle East

Liberalism and democracy are thought to go hand in hand in the West, but as the Arab world begins to experiment with democracy on its own, this concept is being tested. Shadi Hamid, a senior fellow at The Brookings Institution, conducted extensive research of the Muslim Brotherhood in Egypt and Jordan, and he has uncovered that Islamist movements are proving to be illiberal. Hamid presents that the disconnection with the West is rooted in a fundamental misunderstanding of where religion plays in Middle East. In emphasizing this point, Hamid quotes the former leader of the Muslim Brotherhood Abdel Moneim Abul Futouh: "Today those who call themselves liberals or leftists, this is just a political name, but most of them understand and respect Islamic values. They support the sharia and are no longer against it" (Hamid: May 6, 2014a). Furthermore, Western democracy

developed on the foundation of liberal ideals. In the context of Arab democracies, reverse democratization is unfolding where democracy is the foundation for Islamism.

What is a liberal democracy? The discussion of this topic could fill volumes, but to briefly touch upon the subject, liberal democracy is practiced primarily in the West. It is a representative political system which allows for free and fair elections, the rule of law, a separation of powers, and the protection of basic freedoms and liberties such as speech, religion, assembly, and property. Following the Arab Spring, illiberal democracy emerged and "The developing world saw democratically elected leaders using popular mandates to infringe upon basic liberties" (Hamid: May 6, 2014a). Even though elections in places like Egypt and Tunisia were free and fair, the ruling parties attempted to directly impact the political system in way that would weaken opposition to its mandate. As explained in previous sections, the ruling parties attempted to manipulate the existing political system so that it would solidify its power for future cycles.

In the past, the general consensus on Islamist parties was that they would have to moderate their ideology once they would be at the helm of state affairs. Hamid concludes that the opposite is true; democratization does not have a moderating effect on Islamist parties and it does not downplay the importance of their ideology. Hamid references the first Egyptian and Tunisian constitutions as being innately contrary to the values found in the Universal Declaration of Human Rights. Where Western and Arab liberals would undoubtedly agree that there are fundamental universal rights, Islamists reject this. From the Islamist perspective, "The will of the people, particularly when it coincides with the will of God, takes precedence over any presumed international human-rights norms" (Hamid: May 6, 2014a).

Islamists, however, cannot be held solely responsible for the promulgation of their ideological program. The illiberal consensus Hamid speaks of is shared by the mainstream. Islamists are not necessarily committed to introducing a new social order; instead, they are utilizing the state to promote and expand upon standards which the mainstream already holds. Hamid states: "Even those Islamists who have little interest in legislating morality see the state as a promoter of a certain set of religious and moral values" (Hamid: May 6, 2014a). In this regard, Hamid points out, initially the Muslim Brotherhood focused on the individual. The concept focused on the development of future generations to influence the political process through a gradual approach, but the advent of the Arab Spring left this model vastly underdeveloped yielding a sense of urgency to manage the political system from the onset. The development process was short, and it left the Muslim Brotherhood to focus on maintaining power.

Hamid stresses Islamists were interested in using democratic platforms to further their program while maintaining it through the democratic process. Islamist illiberalism was showcased particularly when it faced crises, and rather than moderate their positions, they chose to blame the opposition or call for elections to maintain their mandate. On this point, Hamid makes the comparison to European democratization and how parties like the Christian Democrats had to moderate their positions in order to succeed in elections. For Islamists, moderation is not needed because Islam itself

is not a point of contention within the Arab political context. Hamid further expands on this by revealing that the political spectrum in the Egypt and Tunisia respectively shifted to the right. In quoting a senior Jordanian Muslim Brotherhood official, Hamid highlights that as freedom in the political sphere expands, the public consistently chooses Islam. Furthermore, Hamid concludes "Freedom and Islamization were not opposed but rather went hand in hand" (Hamid: May 6, 2015).

The rise of the Islamist militant group ISIS has called into question whether Islamist groups are heading towards this trend. Hamid notes that most Islamists do not fit into the jihadist camp. They are generally members of mainstream movements like the Muslim Brotherhood whose aim is to work within the system to promote Islamic values: "Islamists do not necessarily harken back to seventh century Arabia" (Hamid: October 1, 2015). Although Islamist may reject the tenets of Salafism, defined above, Islamism itself does not require Islamists to put forward its aims. Hamid cites Indonesia and Malaysia where elements of sharia law are more heavily represented than in the context of their Arab contemporaries. Sharia ordinances in the context of Malaysia and Indonesia have been implemented by secular parties themselves and are met with little resistance from the public. (Hamid: October 1, 2015). This continues to fit into the narrative that Islam is a relevant feature of societies where the majority of the population follow the faith.

Minimizing the role of Islam (of radical Islam) in the political sphere is a major challenge. Even in the case of the Turkish Republic, founded by secular leader Mustafa Kemal Ataturk, showcased the rise of the Islamist movement (headed by the AK Party) and proves that Islam is a force in politics. Hamid emphasizes correctly that "Muslims are not bound to Islam's founding movement, but neither can they fully escape it. The Prophet Muhammad was a theologian, a head of state, a warrior, a preacher, and a merchant, all at once" (Hamid: October 31, 2014b). Furthermore, Hamid discusses the idea of reformation within the Islamic world and compares it to the Protestant Reformation witnessed in Europe. He argues that the Islamic world already had its reformation in late nineteenth century. The reformation yielded Islamic Modernism, the first movement which later would evolve into Islamism. Islamic Modernism attempted to allow Islam to be "safe for modernity" and was a response to "secularism, colonialism, the rise of Europe – but it was also, importantly, a response to the creeping authoritarianism of the late Ottoman era" (Hamid: October 31, 2014b). The movement recognized that the state and state power were a political reality. In the past as it related to matters of Islamic law or governance, the clerical class in Muslim societies maintained a prominent role, and Islamic modernists effectively changed the course of that dynamic for future generations.

As Islam plays a major role in societies in the Middle East, Hamid explains this is where ISIS draws its strength. For example, the idea of having established a "Caliphate" within its territory is a powerful tool in gaining support, even if the masses don't agree with ISIS' interpretation of what the Caliphate is. Seeing a Caliphate evolve resonates in a manner that offers the masses a return to the past or a return to order and greatness. Since the fall of the last true Caliphate in 1924, the Muslim world has had a difficult time creating a "Post-caliphate political model"

(Hamid: October 31, 2014b). Noting the Brotherhood, the caliphate model would prove difficult; instead, they chose to operate within the confines of the political system. Another issue surrounding the implementation of the "Post-caliphate model" harkens back to Islamic Modernist period and its anticlerical bent. Islamism has effectively developed without the aid of clerics, and they are not entirely interested in seeing clerics elevated to lead the movement. Hamid cites the Muslim Brotherhood having an overwhelming majority of supporters and leaders who came from professional sectors in medicine, engineering, and law. In the case of Salafis, who aim to see a return to the era of the Prophet, the role of clerics is even more diminished. They claim that it is because of the clerical establishment's role in expanding scholarship that Islam lost its purity and power. This yields what Hamid calls the "democratization of religion." In short, groups like al-Qaeda and ISIS have profited from the Salafist model. Salafism itself encourages the independent interpretation of the Quran and the life of the Prophet Muhammad without clerical guidance (Hamid: October 31, 2014b).

Testing liberalism in the context of Arab democracy presents many challenges. The conversation has to take into consideration the importance that Islam plays in the public sphere. Shadi Hamid's conclusion on the matter puts forward that what democracy looks like the in the western world may not necessarily be evident in the Middle East. He is correct in displaying that the Arab Spring yielded illiberal democracy driven by Islamist parties. The core factor driving this conclusion is based on how The Arab Street views Islam as being a relevant force in politics. He also highlights the political vacuum left by the dissolution of Caliphate in 1924 as driving a segment of the public to lean towards Salafist ideas. Even though Islam continues to play a role in public life in the region, parties driving their platforms on it have also been faced with challenges, namely the examples of Egypt and Tunisia mentioned earlier. Although Islamists promote illiberalism, Hamid concludes that in order for "The Westphalian system to survive in the region, Islam, or even Islamism, may be needed to legitimate it. To drive even the more pragmatic, participatory variants of Islamism out of the state system would be doom weak, failing states and strong, brittle ones alike to a long, destructive cycle of civil conflict and political violence" (Hamid: October 31, 2014b).

Some Principal Ideas on Cyber-Democracy, Islam, and Democracy

We should expect that the further diffusion of knowledge (knowledge, research, education, and innovation) should have at least in principle the effect of supporting and further progressing processes of democratization. Knowledge society, knowledge economy, and knowledge democracy interplay (Carayannis and Campbell 2009, 2010, 2012, and 2015; Campbell and Carayannis 2013, 2016a, b). Knowledge and good quality knowledge, available for and accessible to more people and larger segments of society, also via platforms or networks that are internet-based,

advance reasoning capabilities of citizens, eventually pushing forward developments that encourage democracy and democratization. Authoritarian regimes, therefore, are being confronted by the following dilemma: Without more knowledge and innovation, it appears not possible to advance economic performance. One the other hand, when more knowledge is being introduced to society, then it cannot be prevented that knowledge will have spill-over effects in the sense of nurturing demands for more democracy. In the long run, it does not appear to be realistic, to advance economy without also advancing democracy and democratization. However, in the short run, the relationship between knowledge and democracy can be complex, meaning that diffusion processes of internet-based knowledge are not necessarily and automatically linked to a fostering of processes of increased democratization (Carayannis and Campbell 2014).

What is the relationship between democracy and Islam in Muslim-majority countries and societies? This certainly represents a sensitive key question. Islam (in Muslim-majority countries) has an influence on society and democracy. However, we are convinced that it is absolutely misleading and in fact wrong to assert that Islam per se is not compatible with democracy or necessarily at conflict with democracy (for a further reading, see Campbell et al. 2012). What appears to be more important is to acknowledge a need for sensitive learning processes in Muslim majority countries, so that a prospective relationship between Islam and democracy can evolve, so that democracy there can progress to developing further to levels of a high-quality democracy. Democracy, as a concept and belief, is wider than a specific religious system (or a specific party-political approach). Within democracy, there must be sufficient space and tolerance, allowing for different religious beliefs (for example Islam, Christianity, and Judaism), but also for secularism and an explicitly nonreligious comprehension and construction of a vision of society. Pluralism and heterogeneity are essential for democracy and for driving quality of democracy. We should not forget that also Europe experienced complex processes of "separation of church and state" for several centuries, leading to the formation of modern democracy. Christian-Democratic parties in Europe represent an innovative example for a development of bringing Christianity into a good political balance with democracy. In the coming years, we should be prepared to expect that also in the Muslim-majority countries a greater diversity in interpretations of Islam will evolve. The global spreading of knowledge (also via the internet) should impose some additional effects.

Religion, religions, and religious systems can try to influence state and state structures directly. Alternatively, religions can influence values and value systems, which then influence political systems, because every political system, also every democracy, is value-based in a pluralistic sense. Such an "indirect effect" of religions on politics may be more preferable or an advantage, since then religions and nonreligions (for example, secular movements) have an impact on the value-base of politics and democracy (see Fig. 1, also for a comparison of scenario one and scenario two). *Every democracy is also value-based. But no particular political party, and no single religion, should have here a position of monopoly.*

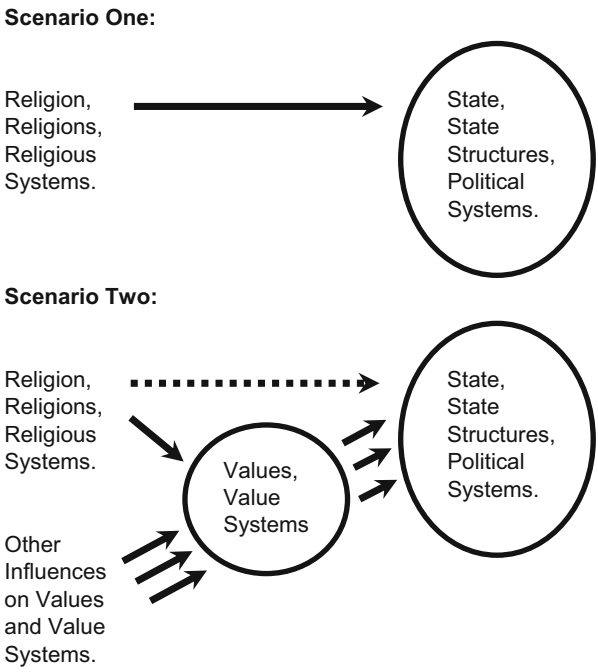


Fig. 1 Possible influences of religion on states, state structures, political systems, and value systems

Conclusion

From the countries of the Arab Spring, so far, only Tunisia managed to follow successfully a path toward more democracy and democratization. By this, Tunisia represents a potential role model for a transformation from authoritarianism toward democracy for the whole region of the Arab countries. A vast majority of the other Arab countries suffered from a decline in levels of modest democracy attempts, when the years 2011–2012 and 2014–2015 are taken as reference points (see for the Democracy Ranking 2016 in more particular Campbell et al. 2017). Tunisia considerably increased in a positive direction its scoring on quality of democracy (see Table 2), while other Arab countries (for example, Egypt, Libya, and Syria) suffered from a further decline in levels of democracy and democratization (for possibilities and options of democracy measurement, see: Campbell et al. 2013, 2015). The latest "Arab Human Development Report 2016", issued by the United Nations Development Program, also indicates several troublesome developments: the "report warns that the policies and practices of exclusion across various fields, the lack of sufficient protection of political freedoms and human rights, weak economic competitiveness and the failure to establish good governance – particularly through greater transparency and accountability – are threatening the future prospects of youth and drawing some into circumstances that hinder their development." Therefore: "This report calls for placing young people at the heart of the development process, which

Table 2 The development of quality of democracy in Core Countries of the Arab Spring (years 2011–2012 and 2014–2015 in comparison). Countries ranked according to scores, Norway serves as a reference country (reference democracy)

	Years 2011–2012	Years 2014–2015	Changes in scores
Norway	99.6	100.0	+0.4
Tunisia	37.1	48.6	+11.5
Egypt, Arab Republic	19.8	15.4	−4.4
Libya	14.8	6.7	−8.1
Syrian Arab Republic	4.3	0.0	−4.3

Methodic note: Scoring spectrum extends from 0 (the lowest observed democracy value) to 100 (the highest observed democracy value). The democracy Ranking 2016 samples and compares 113 countries, and there ranks Norway (2014–2015) the highest, and Syria (2014–2015) the lowest
Source: Authors' own calculations based on the Democracy Ranking 2016 (Campbell et al. 2017)

includes providing young people with genuine opportunities to unleash their energy and shape their future" (United Nations Development Program 2017, p. 17).

In the course of this discussion we have uncovered a great deal of information surrounding the regression of Cyber-Democracy in the Middle East. The conclusion on the future for democracy in the Middle East is still a complicated matter. The region as it is currently trending appears to approach the subject with caution because it is witnessing the pains required to achieve a fruitful democratic transition. Even the data presented offers paradoxes in the vitality of Cyber-Democracy in the coming years. On the one hand, we see a region keeping pace with the digital revolution, yet on the other we see the participants of those revolutions asking for more restrictions on the same platforms used during the Arab Spring. Governmental and elite-driven repression of democratization are one thing, but what has been uncovered here is that even the individual level is responsible for self-inflicted regression. Self-censorship online seems to be taking hold as fewer people believe the internet can effectively develop change. One cannot rule out that the turmoil in conflict zones like Syria, Yemen, and Libya are also impacting public opinion on democratization. Although these conflicts weigh heavily on the Arab Street, it has also proven to be a successful deterrent in the case of Tunisia. The young democracy managed to maintain the course towards democratization because the fear of a Syria-like conflict within Tunisian borders convinced the public to stay the course towards democracy. Illiberalism in the context of an Arab Democracy is also a concern for Western onlookers who have a preconceived notion that democracy and liberalism go hand in hand. In the end, democratization in the Middle East will have to take its course according to its own nature. Even if the current situation offers a picture of regression in Cyber-Democracy or democratization in general, faith in the democratic process now brought to the forefront in the Middle East must yield effective results.

This leads us to developing a preliminary model for an Arab Democracy in the context of the Post-Arab Spring. There are positive models to draw upon and perhaps the Tunisian experience is presenting the most effective example. As far as the Middle East is concerned, two examples of Muslim-oriented democracies are present and continue to operate within the region. The first is Turkey and the second is Iran, but we

must keep in mind that both states are not ethnically Arab nor do they enjoy ethnic or religious homogeneity. The Turkish model was established from the beginning as a secular state and featured a built-in countermeasure from the military to maintain the secular nature of the republic. The introduction of this system by Kemalists was revolutionary from the start and still had complications. Since the creation of the secular Turkish Republic, the Islamist current in the country was equally powerful. The country has reoriented itself towards its Islamic roots under the leadership of President Recep Tayyip Erdogan and the AK Parti. Although the democratic system is still in place in Turkey, the evolution of the state since the Islamists have taken power has produced a state that is still repressive in comparison to Western democracies. The problem in this case was the lack of gradual evolution towards liberal democracy. As a result, the importance of Islam in the political sphere could not be avoided, in less than 100 years the secular identity of Turkey is slowly being reversed. Therefore, the complete removal of Islam in the public sphere cannot be achieved; the inherent prominence of Islam is far too important. In this regard, Kemalists made a miscalculation even though they preemptively aimed to counteract it.

The Islamic Republic of Iran offers a case that Arab democracies should avoid. In the case of Arab countries, the prominent sect is Sunni Islam, where a highly sophisticated clerical hierarchy does not exist as it does in the Shia world. This offers a unique advantage to Arab democracies because it inherently dissolves the concept of theocracy. As previously mentioned, Islamists in Tunisia were very careful to avoid the theocratic systems of Iran and Saudi Arabia when they envisioned the state. If there is to be sustainable and effective governance in Arab democracies, the Iranian model will prove constraining and will lack any possibility of evolution. The Islamic Republic of Iran is a uniquely Iranian concept. A conflict of ideology presents itself as an obstacle for reform, and even with a young population in Iran, overcoming this issue has proved difficult. The ideological struggle is the Islamic Republic refuses to acknowledge Western concepts of liberal democracy and feels that its interpretation of democracy is superior to the west (Litvak 2011, p. 6). Finally, the repressive nature of the Islamic Republic presents more of the same style of regimes Arab countries have faced in the past – they are not interested in reliving them again.

This was apparent with the outcome of the Green Revolution in 2009. Contesting the reelection of the then President Mahmoud Ahmadinejad ruled out any possibility of changing the system in order to orient it towards a Western style democracy. The reality for Iran is that it has a system created through its own political development in the context of its history. We must call to mind, the 2009 opposition candidate Mir Hossein Moussavi was a member of the political establishment, and from his point of view, he was contesting an election he felt was rightfully his. The danger for Arab democracies following the Iranian model is the model forces reformers to operate within a system that does not lend itself to peaceful change. This is evident in light of the violence and turmoil witnessed during the protests. To conclude, the Iranian model proves too rigid to developing a transformation to the system itself (Xavier and Campbell 2014, pp. 163–166).

There are elections taking place in Iran among different contenders, and which are competitive. However, the permitted political spectrum is rather limited and

restricted. Compared with a western-style democracy, this would be as if the only allowed elections would be primaries within the spectrum of a particular political party or political movement (or of "one" political party).

The illiberalism factor must be taken into account when envisioning an Arab democracy. The discussion here boils down to a set of values that are widely held by the mainstream. Even in the case of Western Europe, religion still played a significant role in developing democracy. As Hamid pointed out, Western democracies achieved liberalism prior to democratization, but in the case of the Middle East reverse democratization has taken effect. Looking back at Tunisia and Egypt, we can determine that even if Islamist parties initially take control of the government, their inability to manage the affairs of the state proved ineffective fairly early on. The key miscalculation of Islamists in both cases was meeting the public's real demands: stability and prosperity (Xavier and Campbell 2014, p. 170). This miscalculation opened the door for greater competition among political parties in Tunisia because the Ennahda was at its core willing to step down from power in order to salvage the unity of the state rather than see it spiral into chaos. This is not a solidified victory for leftist or more liberal parties either; the voting public will hold their demands to any future ruling party. Consequently, it may yield potential Islamist victories in the future if leftist and secular parties fail to meet those demands as well.

Political development in Egypt is effectively dominated by the pro-Sisi coalition since the removal of Morsi and the Muslim Brotherhood. The Egyptian parliamentary elections of 2015 further solidified the pro-Sisi coalition with the victory of the "For the Love of Egypt" gaining 20% of seats in the Parliament. Voter turnout in the Egyptian elections was significantly low with 29.83% of eligible voters participating in the second electoral round. In addition, the Salafist Nour Party was virtually decimated in the elections gaining only eight seats in parliament (Aman 2015). As it relates to the development of the Arab democracy model, Egypt's political dynamics were driven primarily by the overthrow of the Muslim Brotherhood. Many question if the military ever really lost control of the situation following the revolution. In a sense, the military preserved the revolution in hopes of achieving stability, but with the advent of the pro-Sisi coalition achieving victory, the president will continue to steer the course of Egypt's political future.

Militant Islamism in the form of Salafist Jihadism presents a double-edged sword for democratic evolution in the region. As it was the case for Tunisia, Islamist parties recognized the threat on the fragile young democracy, but Ennahda appeared weak in confronting it thereby enabling the opposition to criticize their efforts and transition to victory in the polls. Conversely, it also encouraged Salafist groups within the country to take bold stands in presenting a viable option for the public to turn to, but it was a hard sell. The rhetoric of combating this threat is also being used in Egypt. As mentioned earlier, the threat of Salafist groups like ISIS are weighing heavily on the mind of the Arab Street. The public is aware of the destabilizing effect that such a group can have on the state, but just as it can encourage the preservation of the state it can also encourage the mainstream who feel they have a religious obligation to reinstate the caliphate in the region to support it by direct or indirect means. Emerging Arab democracies must be vigilant against the threat of ISIS or face

potential destabilizing effects within their domestic sphere. If ISIS is to intensify attacks against these states as it has in Tunisia and in Egypt in the Sinai it will serve as further justification to maintain added repressive measures in order to maintain safety. Increased attacks from the group may also prove to solidify the resolve of the public to stay the course in democratization, but this effort must be maintained with great caution.

Radical antidemocratic political movements, which assert to be influenced by Islam, pose a serious problem. In theoretical terms, a "caliphate" represents a premodern (in that sense a predemocratic) political concept for the political organization of a state, which does not apply principles of separation of power between the different branches of government in a democratic tradition, but implies a combination and falling-together of political and religious leadership. Caliphates assert to stand in line of a direct legacy and continuation with the establishment and founding of Islam in the early seventh century. When the terror organization of ISIL, the "Islamic State of Iraq and the Levant" (sometimes also being translated as IS or ISIS, "Islamic State of Iraq and Syria"), issued the claim of having (re-) established a caliphate in 2014, in a certain sense a political reality reemerged with connotations now 1400 years old. While other terrorist organizations, like Al-Qaeda, operate more in formats of an underground organization, ISIL is driven by the desire of forming and building state (quasi-state) structures, expressed in the understanding of having set up a caliphate. From an ISIL perspective, only military defeat would drive complete ISIL back into the status of an underground organization.

According to Wieland Schneider (2015), what makes ISIL so distinct and specific are (1) the levels of publicly demonstrated atrocities, (2) the introduction of slavery, but (3) also the way how ISIL managed these approaches in their media propaganda, using social media and videos. ISIL could and does tailor its media messages, depending on and differentiating between media markets, addressing Arab countries or Western societies in various and particular ways (Bösch 2017). For this, Schneider also introduces the term of "Jihadism" as a form of a "bizarre pop culture" (Schneider 2015, p. 213). All of this feeds into the interest of ISIL to build the quasi-state structures of a caliphate, supported and defended by ISIL insurgent groups in the West, so to strike there directly terrorist attacks. Furthermore, ISIL attempts to diffuse into other Arab countries, most notably Libya. In that sense, ISIL may also be interpreted as a fluid spectrum, ranging from underground groups on the one side, over to state building attempts on the other. These state-building efforts of ISIL make ISIL distinct (and draw a line of difference against Al-Qaeda).

We conclude that the model for an emerging Arab democracy must be maintained with a gradualist approach and cannot lose sight of the value democracy offers. In order for democracy to take hold in the Middle East, democratically elected parties must convey to the public that they are making concentrated efforts to provide stability, economic development, the rule of law, and freedom for all people. The concerns of illiberalism being innately part of Islamic democracy is indeed evident, but the transition to liberal democracy will have to run its course and is still a possibility. The key to this development must be directed by the willingness of

political elites, broadcast media, and the individual himself to want it to succeed. Tunisia is a good model for emulation because the core of its progression was based on the determination to see democracy succeed. We must note, even if Tunisia is the only genuine Arab democracy, it is still fragile and must be observed cautiously.

Cyber-Democracy platforms in the Middle East are still a relevant force in the political development of these young democracies, but they are still subject to manipulation and self-degradation. Restricting them may counteract any success that has already been achieved. Regression in this area is a reality, but it could be temporary at best. Militant movements are also hindering the development of political development in the region for reasons outlined extensively in this chapter; the final verdict here must be to see the downfall of such movements. Like any radical movement that has emerged in history, it must be dealt with directly or else it will only gain more strength and influence.

Further observation of the region is still necessary in assessing the impact of Cyber-Democracy in the Middle East. Here are several discussion points. The first, when will Tunisia become a liberal Western style democracy? Are Arab media outlets in need of reform? Is Egypt's President, Abdel Fattah Al-Sisi, intent on transitioning Egypt into a liberal democracy or a semi-liberal democracy? How great is the ISIS impact on preserving further democratization in Egypt and Tunisia? Will the impact of a democratic Tunisia serve as a future model for democratization in the Arab world as a whole? These are several points worth noting and expanding upon in the years to come.

As the region has shifted into the era of the Post-Arab Spring, the prospects for the hope of the seeing the region transition into the "Era of Arab Democracy" is certainly in question. From the perspective of Western observers, few can say that they have witnessed a live democratic transition engulfing an entire region from such a different cultural reference point. We must not be quick to impose Western standards or preconceived notions of democracy upon the Middle East. It has to unfold naturally and gradually, for no western nation-state can say it has not endured great pains to develop its own democratic system.

We want to close our analysis with the vision that, in the long run, democracy and further democratization will finally arrive in the Arab countries on a broader and more durable basis. No other outcome shall be acceptable or shall be accepted. This also aligns with beliefs that democracy and democratic development associate with sustainable development (Campbell and Carayannis 2014; Campbell et al. 2015). *Cyber-Democracy will have here its role, and has all the potentials and capabilities to contribute and* co-co*ntribute to such a desired outcome.*

Cross-References

- ▶ Citizenship Education and New Media: Opportunities and Challenges
- ▶ Libya: Where Cyber-Democracy Reached Its Limits – How the Case of Libya Challenges the Idea of Cyber-Development

References

Al Jazeera journalists freed from Egypt prison (2015, 23 September). Aljazeera. Online article. http://www.aljazeera.com/news/2015/09/al-jazeera-journalists-pardoned-egypt150923112113189.html. Accessed 14 Nov 2015.

Aman, A. (2015, 1 December). Sisi supporters secure second-round elections victory. Online article. Al-Monitor (http://www.al-monitor.com/pulse/originals/2015/12/egypt-parliamentary-elections-president-sisi-supporters.html#). Accessed 15 Dec 2015.

7th Annual ASDA'A Burson-Marsteller Arab Youth Survey (2015). PDF document: Survey. (pp. 6–7, 8, 10, 14, 18, and 26). ASDA'A Burson-Marsteller. http://www.arabyouthsurvey.com/media/document/2015-AYS-White-Paper-EN.pdf. Accessed 30 Sept 2015.

Beissinger, M. R, Jamal, A., & Mazur, K. (2015, 19 October). Online article. What the Arabuprising protesters really wanted. The Washington Post. https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/10/19/what-the-arab-uprising-protesters-really-wanted/. Accessed 1 Nov 2015.

Blair, E., Taylor, P., & Perry, T. (2013, 26 July). Special report: How the Muslim Brotherhood lost Egypt. Online article. Reuters. http://www.reuters.com/article/us-egypt-mistakes-specialreport-idUSBRE96O07H20130726. Accessed 22 Nov 2015.

Bösch, P. G. H. (2017). *Der "Islamische" Staat: Kalifat des Schreckens? [the "Islamic" state: Caliphate of scare?]*. Vienna: Manuscript.

Campbell, D. F.J., & Carayannis, E. G. (2013). Epistemic governance in higher education. In *Quality enhancement of universities for development (SpringerBriefs in Business)*. New York: Springer. http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6

Campbell, D. F. J., & Carayannis, E. G. (2014). Explaining and comparing quality of democracy in quadruple helix structures: The quality of democracy in the United States and in Austria, Challenges and opportunities for development. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 117–148). New York: Springer. http://link.springer.com/chapter/10.1007%2F978-1-4939-1028-1_4

Campbell, D. F. J., & Carayannis, E. G. (2016a). Epistemic governance and epistemic innovation policy. *Technology, Innovation and Education, 2,* 2, 1–15. https://doi.org/10.1186/s40660-016-0008-2. http://technology-innovation-education.springeropen.com/articles/10.1186/s40660-016-0008-2

Campbell, D. F. J., & Carayannis, E. G. (2016b). The academic firm: A new design and redesign proposition for entrepreneurship in innovation-driven knowledge economy. *Journal of Innovation and Entrepreneurship, 5*, 12, 1–10. https://doi.org/10.1186/s13731-016-0040-1., http://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-016-0040-1

Campbell, D. F. J., Barth, T. D., Pölzlbauer, P., & Pölzlbauer, G. (2012). *Democracy ranking (edition 2012): The quality of democracy in the world*. Vienna: Democracy Ranking (Books on Demand), Vienna. https://www.amazon.com/Democracy-Ranking-Edition-David-Campbell/dp/3848217988/ref=sr_1_22?ie=UTF8&qid=1349340296&sr=822&keywords=Campbell%2C+David+F+J%20and%20http://www.amazon.com/Democracy-Ranking-Edition-2012-ebook/dp/B009KVQ19E/ref=sr_1_12?ie=UTF8&qid=1349346706&sr=812&keywords=Campbell%2C+David+F+J%20and%20http://www.amazon.de/Democracy-Ranking-Edition-2012-Quality/dp/3848217988/ref=sr_1_6?ie=UTF8&qid=1357199668&sr=8-6

Campbell, D. F. J., Carayannis, E. G., Barth, T. D., & Campbell, G. S. (2013). Measuring democracy and the quality of democracy in a world-wide approach: Models and indices of democracy and the new findings of the "Democracy Ranking". *International Journal of Social Ecology and Sustainable Development, 4*(1), 1–16. http://www.igi-global.com/article/measuring-democracy-quality-democracy-world/77344

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: the USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493. http://link.springer.com/article/10.1007/s13132-015-0246-7

Campbell, D. F. J., Pölzlbauer, P., & Barth, T. D. (2017). *Democracy ranking 2016*. Vienna: Democracy Ranking Organization. http://democracyranking.org/wordpress/

Carayannis, E. G., & Campbell, D. F. J (2009). "Mode 3" and "quadruple helix": Toward a 21st century fractal innovation ecosystem. *International Journal of Technology Management, 46*(3/4), 201–234. http://www.inderscience.com/browse/index.php?journalID=27&year=2009&vol=46&issue=3/4 and http://www.inderscience.com/search/index.php?action=record&rec_id=23374&prevQuery=&ps=10&m=or

Carayannis, E. G., & Campbell, D. F. J. (2010). Triple helix, quadruple helix and quintuple helix and how do knowledge, innovation and the environment relate to each other? A proposed framework for a Trans-disciplinary analysis of sustainable development and social ecology. *International Journal of Social Ecology and Sustainable Development, 1*(1), 41–69. http://www.igi-global.com/bookstore/article.aspx?titleid=41959

Carayannis, E. G., & Campbell, D. F. J. (2012). *Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development (SpringerBriefs in Business.).* New York: Springer. http://www.springer.com/business+%26+management/book/978-1-4614-2061-3 and http://www.springer.com/cda/content/document/cda_downloaddocument/9781461420613-c1.pdf?SGWID=0-0-45-1263639-p174250662

Carayannis, E. G., & Campbell, D. F. J. (2014). Developed democracies versus emerging autocracies: Arts, democracy, and innovation in quadruple helix innovation systems. *Journal of Innovation and Entrepreneurship, 3*, 12. http://www.innovation-entrepreneurship.com/content/3/1/12

Carayannis, E. G., & Campbell, D. F. J. (2015). Art and artistic research in Quadruple and Quintuple Helix innovation systems. In G. Bast, E. G. Carayannis, & D. F. J. Campbell (Eds.), *Arts, research, innovation and society* (pp. 29–51). New York: Springer. http://link.springer.com/chapter/10.1007/978-3-319-09909-5_3

Dennis, E. E., Martin, J. D., & Wood, R. (2013). Media use in the Middle East: An eight-nation survey. PDF document: Survey, (pp. 8, 11, 15, 17, 36, 24–25, 34, 59–60, 55–56, and 95). Northwestern University in Qatar. http://www.qatar.northwestern.edu/docs/2013-Media-Use-Middle-East.pdf. Accessed 30 Sept 2015.

Egypt Court Bans Muslim Brotherhood's Political Wing. (2014, 9 August). Online article. BBC. http://www.bbc.com/news/world-middle-east-28722935. Accessed 15 Dec 2015.

El Deeb, S. (2013, 30 December). Egypt Arrests Al-Jazeera Journalists Amid Muslim Brotherhood-Crackdown. Associated Press. Online article. Huffington Post. http://www.huffingtonpost.com/2013/12/30/egypt-arrests-al-jazeera-journalists_n_4517884.html. Accessed 15 Nov 2015.

Freedom on the Net 2014: Egypt. (2014). Freedom House. PDF document, (pp. 260 and 259). https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf. Accessed 30 Sept 2015.

Freedom on the Net 2014: Tunisia. (2014). Freedom House. PDF document, (p. 783). https://freedomhouse.org/sites/default/files/FOTN_2014_Full_Report_compressedv2_0.pdf. Accessed 30 Sept 2015.

Freedom on the Net 2015: Egypt. (2015). Freedom House. PDF document, (pp. 270 and 268). https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf. Accessed 30 Sept 2015.

Hamid, S. (2014a, 6 May). The future of democracy in the Middle East: Islamist and illiberal. Online article. The Atlantic. http://www.theatlantic.com/international/archive/2014/05/democracys-future-in-the-middle-east-islamist-and-illiberal/361791/. Accessed 30 Sept 2015.

Hamid, S. (2014b, 31 October). The roots of the Islamic State's appeal: ISIS's rise is related to Islam. The question is: How? Online article. The Atlantic. http://www.theatlantic.com/international/archive/2014/10/the-roots-of-the-islamic-states-appeal/382175/. Accessed 21 Oct 2015.

Hamid, S. (2015, 1 October). What most people get wrong about political Islam. Online article. The Brookings Institution. http://www.brookings.edu/blogs/markaz/posts/2015/10/01-what-people-get-wrong-about-political-islam-hamid. Accessed 21 Oct 2015.

Internet World Stats. (2015). Internet users in the Middle East November – 2015. Internet World Stats: Usage and population statistics. Web Resource accessed, 3 Apr 2016. http://www.internetworldstats.com/stats5.htm

Kandil, H. (2014, 27 February). The Muslim Brotherhood failed in Egypt because it was inept, incompetent and out of touch. Online article. Chatham House Journal, The World Today via The Conversation. http://theconversation.com/the-muslim-brotherhood-failed-in-egypt-because-it-was-inept-incompetent-and-out-of-touch-23738. Accessed 22 Nov 2015.

Litvak, M. (2011). Iran: Prospects and obstacles to democratization. *The causes and consequences of democracy: Regional and global perspectives* (pp. 1–13). Stanford University Department of Political Science. Moshe Dayan Center for Middle Eastern and African Studies Tel Aviv University. Web. 16 April 2013. https://politicalscience.stanford.edu/causes-and-consequences-democracy

Lynch, M. (2015). After the Arab Spring: How the Media trashed the transitions. PDF document. *Journal of Democracy, 26*(4), 91–97. http://www.journalofdemocracy.org/sites/default/files/Lynch-26-4.pdf. Accessed 1 Nov 2015.

Marks, M. (2015). Tunisia's Ennahda: Rethinking Islamism in the Context of ISIS and the Egyptian Coup (Working Paper). Washington, DC: The Brookings Institution. https://www.brookings.edu/wp-content/uploads/2016/07/Tunisia_Marks-FINAL_2.pdf

Radsch, C. (2015, 27 April). Treating the Internet as the enemy in the Middle East. Committee to Protect Journalists (CPJ) https://cpj.org/2015/04/attacks-on-the-press-treating-internet-as-enemy-in-middle-east.php. Accessed 30 Sept 2015.

Salvatore, A. (2013). "Before (and after) the 'Arab Spring': From connectedness to mobilization in the public Sphere|Armando Salvatore – Academia.edu." *OrienteModerno* XCI.1 (2011), 5–12. Academia.edu. Web. 16. http://www.academia.edu/1416964/Before_and_After_the_Arab_Spring_From_Connectedness_to_Mobilization_in_the_Public_Sphere

Schneider, W. (2015). *Krieg gegen das Kalifat. [war against the caliphate]*. Vienna: Braumüller.

United Nations Development Program. (2017). *Arab human development report 2016: Youth and the prospects for human development in changing reality*. New York: United Nations. http://arab-hdr.org/PreviousReports/2016/2016.aspx

Xavier, R. F., & Campbell, D. F. J. (2014). The effects of cyberdemocracy on the middle east: Egypt and Iran. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice* (pp. 147–173). New York: Springer. http://link.springer.com/chapter/10.1007/978-1-4939-1028-1_5

Democratization in the Middle East and North Africa: Tunisia, Egypt, and Turkey

32

Tuğba Özcan

Contents

Abstract

This paper deals with the question of democratization in the Middle East and North Africa in recent years. The chosen examples are Tunisia and Egypt for the so-called Arab Spring and Turkey because it very often serves as a model for democratization in the Middle East on the one hand and the marriage of democracy and Islam on the other hand. Furthermore, due to its geographical and historical-cultural location, it serves as the interlocutor between east and west. A specific focus in the paper will be given to the role of new media in the protests for and the process of democratization.

T. Özcan (✉)
Master of Arts in Political Science, University of Vienna, Vienna, Austria
e-mail: tuba_oezcan@hotmail.com

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_8

Keywords
Arab Spring · Democratization · Egypt · Middle East · North Africa · Revolution · Social media · Tunisia · Turkey

The Process of Democratization in Tunisia and Egypt

Introduction

The Arab Spring is a historical turning point in the region entailing widespread political, economical and geostrategical condequences (Cited after Kreft 2011).

What began in Tunisia in December 2010 spread out like a wildfire into many countries of North Africa and the Middle East. Protests and uprisings shattered the foundations of the autocratic systems in the region. In Tunisia and in Egypt, the protesters drove the rulers out of office.

Even though there has been a lot of talk about "Arab Revolutions" recently, which supposedly have numerous socioeconomic and political factors in common, one cannot speak of one Arab Revolution (cited after Kreft 2011: "that these movements – contrary to common opinion – were no complete surprise to careful observers of the developments in the Middle East has to be clearly stated. The analyses of the 'Arab Human Development Report' published by the UNDP every year since 1995, have been pointing out the grave social and political deficits of the Arab states for more than a decade. These were unfortunately hardly perceived by the rulers in the Middle East."). The respective national circumstances are too different in the single states generally subsumed under that label, just as the chosen strategies to overthrow dictatorial regimes, which themselves were completely different in character, varied as well (see Kreft 2011).

It is thus no surprise that the first of those movements, namely, those in Tunisia and Egypt, came closest in character to genuine grassroots movements. Especially in the case of Tunisia, and also Egypt, one can speak of democracy movements, which were first and foremost carried by a hopeless and frustrated youth. The chosen methods concurred for the most part with the methods of nonviolent resistance and democracy movements. A major factor for their relative success was the moment of surprise, for they literally caught the dictators and their repression machines "on the wrong foot." Another major factor was that the interventions of foreign powers which accompanied the subsequent "revolutions" were not practiced in such a way in those two cases mentioned above.

Theses on the Development of the Arab Spring

- The rentier states and the allocation regimes, as well as the politics of the US and the EU directed at supposed stability, strengthened authoritarian structures, which blocked those states from developing politically and economically in the long run.
- The protest movements and revolutions in the Arab world are not only pure democracy movements but also economic struggles of distribution, under conditions sharpened by the world financial crisis.

- Those struggles of distribution are either to be resolved in the form of successful revolutions and social redistribution, for which there still has to be fought in Egypt and Tunisia, or to be led in long-term violent struggles of distribution.
- Democracy and social justice are unthinkable without gender equity. The participation of women in the protest movements has so far not guaranteed a stronger position of women after a revolution. Especially in heavily patriarchal societies, the question of gender becomes a central issue for the success of democratic and social movements.
- Such violent struggles of distribution can lead to a confessionalization and tribalization of conflicts in societies without a sufficiently developed urban population and class society. In such a case, a deterioration into a long civil war up to a near complete failure of the state is possible.
- In such conflicts international intervention can entail a wide range of different consequences. The activity of key states in the region, such as Iran or Saudi Arabia, is therefore to be analyzed as detailed as the European and US American actors.
- The protest movements are not to be viewed as isolated Arabic phenomena but as part of the increasing global conflicts of distribution, which are a consequence of the neoliberal economic policy of the last 40 years and especially of the economic crisis since 2008.

In fact, the struggles about the distribution of the effects of the crisis and the distribution of resources intensified not only in the Arab world. These struggles can be solved through political struggles and solidarity from below, or they can lead to military conflict and civil war along ethnic, national, religious, or tribal limits. Despite Tahar Ben Jelloun's hope that "never again a dictator will be able to stomp on the dignity of the Arabic people" (Preiss 2013; cited after Ben Jelloun 2011, p. 91), the alternative to dictatorship is not always a democracy, but sometimes another dictatorship or the permanent disintegration of a society. Without a changing of the economic basis, a democratic development of the Middle East and Northern Africa is hard to imagine. More than ever, and not only in the Arab world, the alternative formulated by Rosa Luxemburg 100 years ago is pertinent: "Socialism or Barbarism!" (Preiss 2012, p. 221 cf).

The "Arab Spring": A Spring of Democracy?

In the following I briefly display the different theoretical approaches to the question of democratization as analyzed by political scientist Wolfgang Muno. The structuralist approach of modernization theory supposes an increasing wealth and prosperity and a consequently following emergence of a middle class through modernization. This approach concludes that thereby the development of democracy is fostered. Judging from their GDP/capita, the Arab states are relatively wealthy. The cultural theory on the other hand supposes that neopatrimonial political systems find their expression in patriarchal social structures with mainly informal ways of decision-making. *This is to be viewed in the*

context of the question if Islam with its societal structure is compatible with democracy in general. It is also evident that not necessarily Islamic countries in general, but Arabic countries show little signs of a democracy, analyzes the Wolfgang Muno. The structural theory on the other hand aims at the power structures of the rentier economy. In the Arab countries rich in resources just as in those poor in resources, there is a repeated adjustment and assistance, if the state is not able to provide an adequate allocation of means. Thus rentier economies emerge, which are not genuine economies, but consist of a large overblown bureaucratic apparatus and generally a large overblown security apparatus as well, which is supported by foreign help. Wolfgang Muno (cited after Mainz 2012) states that "without a tax system there is no mutual dependence between the citizens and the state ('no taxation without representation')" (Ebd.). The rationalistic approach of the actor theory is based on the view of the political actors and their categorization in elites, counter-elites, and masses.

> The different stages of democracy Dr. Muno sketches and displays with the catchwords listed below: liberalization, demoralization, transition and consolidation. Regarding the transition taking place in the Arab world right now he classifies some countries of the region according to the following categories:
>
> - United elite – repression – oppression of the masses (Bahrain)
> - United elite – repression – civil war (Libya, Syria)
> - United elite – liberalization from above – changes in the regime (Morocco, Jordan)
> - Split elite – alliance of liberal reformers and masses – regime change (Tunisia, Egypt) (cited after ibid.)

Many of the affected countries, says Muno, are very young: 65–75% of the population are younger than 35 years. The peer group of those born between 1975 and 1990 constitutes roughly 30% of the population in the region. Additionally, this is the generation with the highest degree of education on average, and thus they are very well versed in the use of new media. At the same time, however, these young people are excluded from the participation in the rentier economy to a large extent, and they feel excluded from political participation in general. The concept of "revolution post-Islamist" consequently does not mean the demand for more Arab nationalism or Islamism. The debates over which form of democracy should be desired have to be fought out according to local criteria, which will, according to Wolfgang Muno, entail many problems, i.e., the rule of law, even in a formally democratic state. "The careful prognosis would be that at best there will be a fall. A liberal democracy like in the West is likely off the charts, but a democracy with an Islamic touch is possible" (cited after ibid.).

Revolution

After the Tunisian President Zine El-Abidine Ben Ali had to flee the country in a hurry after week-long protests on January 14, 2011, the successful revolution in

Tunisia became an inspiration for the anger that has been brewing under the surface in Egypt for years. The European and American media as well started to realize that the dissatisfaction of the youth, the students, and the workers in the Arab world was not only a specific regional case but a widespread phenomenon. After the massive protest hit the street and the army forced long-term Egyptian President Hosni Mubarak to step down only a month after Ben Ali's flight, the international media began to talk about an *Arabic 1989*. Connected to this designation was the understanding of the revolutions as "democratic liberal revolutions." Those who opposed to such an understanding were evoking the specter of an "Islamic Revolution."

Both comparisons fall short, however. A chain reaction in the sense of a collapse of all authoritarian systems in the region did not occur, because, in contrast to the sphere dominated by the Soviet Union, the region was not a unified power block; rather it was an assembly of different authoritarian ruling systems, which did not implode all in the same form, contrary to the Moscow-dominated Eastern European satellite states in 1989. In addition to that, one can witness that the protest movements in Libya, Syria, or Bahrain were not as successful as their counterparts in Tunisia or Egypt.

Also, the comparison with the democratic revolutions in Eastern Europe falls short but for a different reason, namely, because the reason for the revolution and the goals of the heterogeneous opposition movement did not end with democratic and liberal demands, but were closely knit to social demands. Especially the first two successful revolutions in Tunisia and Egypt were also directed against the results and effects of 20 years of neoliberal politics of deregulation. The argument put forth by Emmanuel Todd, who understands the revolution as a consequence of demographic developments (Preiss 2012; see Todd 2011), undervalues the economic development, and allows a biologicization of the unfolding events.

Characterizing the revolutions as anti-neoliberal in a broad sense can also explain the broad alliances, spanning from the organized left, and unions to an ideologically loose youth to factions of Political Islam.

The authoritarian welfare states had, in the 1960s, promised the working class and the country population and peasantry the possibility of a social advancement into the middle class, but these hopes were crushed by the economic deregulation from which mostly the capital factions associated with the regime profited. The hope for a social advancement formed the core of what in political science is often called "authoritarian bargain." This is the undeclared arrangement between the regime and the population according to which the people exchange their political freedoms for a relatively secure social status in the welfare state.

The Swedish political scientist Jan Teorell argues that in times of economic crises this "authoritarian bargain" is increasingly under pressure: "declining economic conditions and corresponding pressures for policy adjustment potentially disrupt the authoritarian bargains forged with all three, thus creating a more hospitable environment for democratization" (Teorell 2010; cited after Preiss 2012, p. 70).

A government which cannot fulfill its duty in this bargain any longer, when an economic crisis hits, is put in question when all illusions about a potentially better future are destroyed and a whole generation of young people can no longer be integrated into the labor market. If this happens, the possibility of founding a family

– that is, to say in conservative Islamic countries very often the possibility of legitimate sexuality – becomes impossible.

Domination always requires a certain, even if only small dose of acceptance by the dominated. This is why the disappearance of this acceptance is decisive for the overthrow of authoritarian regimes. The American political scientist Gene Sharp dealt extensively with the possibility of nonviolent action to overthrow authoritarian regimes and his book *From Dictatorship to Democracy* written for the democracy movement in Myanmar inspired several democracy movements in Eastern Europe and also the movement in Egypt. He views as the central task of a successful democracy movement this disappearance of the acceptance of the regime and the access to the "sources of political power."

> *Without access to the sources of political power 'the dictators' power weakens and finally dissolves. Withdrawal of support is therefore the major required action to disintegrate a dictatorship*. (Sharp 2010; cited after Preiss 2012, p. 67)

Sharp lists the following sources of political power, the access of the regime to which should be cut of:

- "*Authority*, the belief among the people that the regime is legitimate and that the people have a moral duty to obey it
- *Human resources*, the number and importance of the persons and groups which are obeying, cooperating, or providing assistance to the rulers
- *Skills and knowledge*, needed by the regime to perform specific actions and supplied by the cooperating persons and groups
- *Intangible factors*, psychological and ideological factors that may induce people to obey and assist the rulers
- *Material resources*, the degree to which the rulers control or have access to property, natural resources, financial resources, the economic system, and means of communication and transportation
- *Sanctions*, punishments, threatened, or applied, against the disobedient and noncooperative to ensure the submission and cooperation that are needed for the regime to exist and carry out its policies" (Sharp 2010; cited after Preiss 2012, p. 18f)

The basis however is the end of the "authoritarian bargain," which occurred in the recent economic crisis. The revolutions in Tunisia and Egypt were not achieved solely by democracy activists, but they had popular support by the masses because of the increasing inability of the regime to provide its part in the said bargain, which is to provide economic and social security, which can be "traded" for political freedoms.

The protests in Tunisia, which stood at the beginning of the wave of change, connected social and democratic demands from the outset. Starting out as a movement of unemployed and poor, several unions and a large part of the youth soon joined the protest. The revolution in Tunisia is thus to be understood not only as a democratic revolution but closely tied to the economic development of the country.

In Tunisia as well as in Egypt, the overthrow of the government was achieved without driving the country into a civil war or causing massive ruptures in society. The Tunisian and the Egyptian state remained largely untouched, while the regimes were overthrown or transformed (see Preiss 2012, p. 207).

The Success of the Tunisian Revolution

The Tunisian economy was generally speaking on a relatively good path forward. In 2011, the year of the revolution, it shrank 1.8%, which was the first time since 1986. Many jobs have been lost since; even with renewed growth, this tendency did not stop. The Tunisian population is among the best educated in Northern Africa. Yet the economy tended to create jobs mostly for unskilled workers and in the low-wage sector. Unemployment among academics is at 35% and thus almost twice as high as among less qualified Tunisians. This leads to an increasing polarization in the Tunisian society, because several social groups feel excluded from the system. The economic downturn also hit very hard on the Tunisian slum dwellers, the number of which had decreased by 50% before. Even the close ties to the EU could not stop the downward tendencies of the economy. Furthermore the revolution lead to a massive decrease in tourism at the Mediterranean coast (see Pott 2012, p. 124).

The Egyptian Revolution

In Egypt, the political change is very often described as a military coup d'etat. The army certainly played a major role in the – compared to other countries in the region – relatively peaceful turn of events. A decisive fact, however, is that the army leadership reacted much more to pressure from the street than it actively acted itself. The slogan "the army and the people hand in hand" was a central slogan of the protest movement not without reason. What is revolutionary in this is that the street was declared a political space which could now heavily influence political decision-making.

There are many, internal and external, reasons for the Egyptian revolution. Very often both are interdependent. In any case, the events in Egypt cannot be viewed separately from international developments. Sharp's elaborations are a major contribution to the analysis of the political change we are witnessing in the Middle East and North Africa. We should, however, not overlook that Sharp draws a very static picture of dictatorships and democracies, respectively. Democratization can only too easily be understood as a linear process, at the end of which tyrannical or dictatorial regimes are surpassed. The ideal are Western democracies. Democracy, however, is not a good that can be exported and implemented according to external criteria. The formation of public opinion and the influence of external dynamics should not be overlooked. The theses of Sharp are therefore not universal and not easily applicable to the situation in Egypt without further reflection (see Preiss 2012, p. 34).

A Broad Political Spectrum Becomes Visible

During the revolution and after the consensus the whole breadth of the political spectrum became increasingly visible. An increase in potential conflictual situations,

between the old ruling powers and various interest groups, and also between various interest groups themselves, is to be expected. For an analysis of these potential conflicts, one has to draw attention to certain important factors:

- Oppositional groups generally do not have the necessary structures to be successful in democratic elections. Many, especially the Egyptian left, thus demand a longer phase of transition to enable these newly formed or newly empowered forces to strengthen their stance.
- The only oppositional group to have the resources for a successful electoral campaign is the Muslim Brotherhood. Therefore it is in their interest to have elections as soon as possible. This fosters a new alliance between parts of the Muslim Brotherhood and parts of the old ruling classes, especially the army.
- Parts of the old bureaucratic class, to which a certain proximity to the regime of Mubarak can be ascribed, also push for a soon election, in order to keep their old power. They especially point to economic questions and the problem of security that arose in the months after the revolution.
- Social questions become pertinent. Many people, who originally supported the revolution, wanted first and foremost two things: "Bread and Dignity" (El-Gawahry 2011; cited after Preiss 2012). If the fundamental needs of the Egyptian people can no longer be fulfilled, this can lead to a strong desire for the "status quo ante." Many left politicians and activists, however, demand that social questions are to be left aside at first in order to push the process of revolution forward and create the necessary institutional basis for a democratic Egypt after Mubarak.

Is a Democratic Development Possible?

In Egypt and Tunisia, a development toward democracy seems most likely, because in these countries, there is a strong middle class and established state institutions. The democratization moves forward slowly, however, and the voices complaining about the slow process of reforms are increasing in number. Except for the trials against Mubarak, two of his sons, and minister of finance Youssef Boutros-Ghali and former minister of the interior Habib el-Adly not much has happened that merits the designation "reform." The question now is who is responsible for that.

The Islamists participated relatively late in the demonstrations and were visibly careful in the revolution. The military council, however, has a key function, and it seems to tie constantly close relationships with the Islamists. Islamist groups have clearly stated that they want to change the constitution, while the military has so far been silent about this issue and about its goals in general. More importantly, the army has not yet specified when it will withdraw from power, and in fact this withdrawal becomes more and more unrealistic.

The military council wants to set the date for the constitutional reform and the elections and increasingly restricts the freedom of speech. It threatens and tries critics in military courts; there are even reports about the imprisonment of bloggers (cited after Preiss 2012: "Thus the military council freed Colonel Aboud al-Zomor,

'the mastermind behind the Sadat assassination', however, it imprisoned the liberal Egyptian blogger Maikel Nabil Sanad on March 28th 2011 and sentenced him to three years in military prison because of his critique of the military government." (Cynthia 2011), accessed on August 17th 2011), journalists, artists, human rights activists, and activists. Those criticizing the military council and calling for a continuation of the protests (cited after Preiss 2012: "It is said that there have already been 5000 people sentenced by military courts, says Amira El Ahl in *Die Revolution zuerst*' (*The Revolution First*). Muslim Brothers, Salafists and young mavericks are unified by the anger towards the military council which, because of diffuse decrees and delays of trial, have lost their credit with the people." *Die Welt,* July 11th 2011, p. 7) were chased down and in some cases even tortured. This is why there is a growing dissatisfaction over the fact that only the top of the power pyramid has been changed, and now the process of changes has stagnated.

The military council allows no insight in its own power structures, rather the transitional government seems to move all the more toward a military dictatorship. Are these the signs of the new freedoms? Since 1952, all presidents came from the ranks of the army. The army dominates a huge economic empire and has only recently passed a law that all accusations of corruption in the military are only being investigated by the military itself. The army dropped Hosni Mubarak but not its own power. Nobody knows what the military council really wants, because it allows no insight from the outside into its own power structures (Ehrhardt 2011) and decision-making. Yet in the process of democratization, it would be necessary to investigate the role of the army regarding the misuse of power, corruption, and torture during the last 30 years. Also, no movement has been made to hold those accountable who are responsible for the 850 deaths during the revolution.

The Muslim Brotherhood formed the *Party for Freedom and Justice* (PFJ) already in April 2011, which is supposed to be not a religious but a secular party in character. They emphasized repeatedly that a Christian, Rafiq Habib, would be part of the leading council and the party program emphasized that the rights of non-Muslims are to be respected, and even though Sharia law is the dominating principle in Egypt, it should be adjusted to societal developments. Islam is the state religion and the *leitkultur* (see Croiteru 2011, p. 87), but the party does not want to find an Islamic state but a constitutional state.

The leader of the youth faction of the Muslim Brotherhood, Ahmed Akil, made the following statement: "We know that many Egyptians are afraid of us [...] To calm them down we set very modest goals" (Preiss 2012; cited after Gerlach 2011, p. 87). Is the party a democratic party with Islamic orientation? How will it relate to freedom of the press? It is hardly imaginable that the party would change anything about the importance of the Sharia issued in the old constitution.

The Muslim Brotherhood appears to avoid being mentioned in a prominent place, yet, with roughly 30% followers, it will try to claim its part of power. Presumably that will have to be done in a coalition with other groups, either with the help of the military council or with the support of the Salafists. (The Salafists demand the introduction of the Sharia, including the corporate body, they refute a secular state.) Mohammed Badie, the leader of the Muslim Brotherhood, declared as the

goal 50% of the seats in parliament and the introduction of Sharia law (see Windfuhr 2011). What many Egyptians demand in the repeated demonstrations is, however, a secular state and a constitution based on civil society and especially that the army steps down from power. Thus, the principal conflicts are still far from being solved.

The situation in Tunisia is somewhat different in many regards: 69-year-old Rached al- Ghannouchi, living in exile in London for a long time and the founder of the Islamist Ennahda movement, returned to Tunisia. Al-Ghannushi is a colorful personality, who on the one hand praises the jihadist theology of Yusuf al-Qaradawi – who also supports suicide attacks – and once issued positive statements about Sharia law and Hamas, as well as defended the legitimacy of suicide attack, but on the other hand supports democracy, pluralism, and division of powers. In a recent interview, he said, "the Tunisian state is an Islamist state [. . .] Islam is a source of our constitution and an inspiration for the legislator and the fathers of our constitution" (Ghannouchi 2011, cited after Preiss 2012, p. 86).

The Arab World Needs More Democracy: A Comparison of Tunisia and Egypt

The mass protest in the Arab states surprised the respective rulers and the international community. Nonetheless at least experts had, over the course of the last years, pointed toward demographic and socioeconomic developments and thus to the rise in revolutionary potential. In nearly all countries of the Arab world, young people make up a large part of the population; unemployment is soaring (especially among the youth), and the risk of poverty is widespread. Additionally, there is political stagnation coupled with endemic corruption and restrained civil rights and freedom of press.

Within a few days, an increasing number of middle class youth with good education but without perspectives has transgressed its fear from repression from state violence in Egypt and Tunisia. After decades of authoritarian rule, they demanded economical, political and social participation, individual freedoms, good governance, and a constitutional state. The respective flights of Tunisian President Zine el-Abidine Ben Ali and Egyptian President Hosni Mubarak changed many things: in both countries there is independent media; we witness a lively political debate between Islamists and secularists and between conservatives and liberals about a new constitution.

There is a widespread consensus among the varying political camps on the question that a strong legislative power and a restriction of executive power and independent justice, human rights, bourgeois freedoms and a harmonizing social policy are of paramount importance. The Egyptian and Tunisian society have become considerably more pluralistic, while the radicalization feared by many especially in Europe was no major factor. In order for a transformation of an authoritarian regime to a democracy, several important steps have already been taken. The best chances for a consolidation of the process of democratization exist in Tunisia, which is, compared to Egypt, confessionally and ethnically more homogeneous. Furthermore, Tunisia has a well-educated middle class, and the economy and the state institutions are comparably efficient. Egypt, with its 83 million inhabitants about eight times as populated, is

religiously and ethnically much more heterogeneous and faces much bigger socioeconomic and institutional tasks – one of which is the question of the future role of the army. The developments in Egypt and Tunisia as a vanguard of the "Arab Spring" are observed closely everywhere in the Arab world and beyond. Should the consolidation of a participatory democracy directed at social participation be successful in these countries then this would have massive consequences for the whole region. *The process of democratization in Egypt and Tunisia* depends fundamentally on the societal and international framework, because the transitional governments still face the same socioeconomic problems like their autocratic predecessors. Even worse, because of the revolutions, the economy suffered considerably in both countries, the tourist industry collapsed, strikes lead to a loss of production, and domestic and foreign investors are very careful because of the unstable situation. In order to find work for the many unemployed and the migrant workers returning from Libya, the Egyptian government has decided to employ a million people in the public sector, which is completely overloaded anyway. This and the exclusion from tax exemption for the reeling tourism industry contribute massively to state debt. Because of all this, the credit worthiness of the country suffers. Egypt has to pay an annual billion of US dollars to the EU states. The rejuvenation of the economy and the creation of job especially for people under the age of 25 are important conditions for the success of the democratization.

Tertiary education is equally important for the process of democratization. The foundations for an efficient and competitive economy as well as for a democracy based on broad participation are built there. Besides that a democracy needs appropriate institutions, which have to be built, against the forces of the old regime just as against forces hostile to democracy. Whatever the "Arab Spring" can become, more jobs, more education, and more democracy are necessary. Regarding the difficult initial position, it is hard to imagine that the transitional government can be successful in all three aspects over a longer period of time without extensive support from the international community – and even with foreign support success is by no means guaranteed (see Kreft 2011).

The Importance of Social Media in the Arab World

The social media platform Facebook, first online in September 2006, connects over 550 million people worldwide and allows them to keep in touch with their friends and acquaintances and share information. Besides entertainment, platforms such as Facebook, Twitter, or YouTube are increasingly used for political purposes (see Milz 2011).

"During the Arab Spring 2011, the internet and especially social media assumed an exceptional role. The designation 'Twitter or Facebook Revolution' for the political changes in Tunisia and Egypt was ready at hand. Not only in the public and the political debate but also in political science itself, a stance with high expectations, assigning the new media a positive effect for democracy, was common. Autocracies would be increasingly threatened by such interactive forms of

communication and the thus more effective and quicker possibility of mobilizing protest and resistance" (cited after Kneuer and Demmelhuber 2012). "There are also those voices, however, who warn of being too quick to judge and who point to different factors of political change" (cited after Kneuer and Demmelhuber 2012; Rafal: Liberations. Control in Cyberspace, in: Journal of Democracy 4/2010, pp. 43–58.). Since the events in the Arab world, we are witnessing a lively debate in politics, media, and science on what new media and especially Web 2.0 media is capable of achieving in respect to political processes of change and what the relevance of classical media is in such processes (see Kneuer and Demmelhuber 2012).

The Role of Social Networks in Tunisia

Social Networks were highly relevant in Tunisia already before the revolution. Through WikiLeaks information about corruption in Tunisia was made public. This massively increased the discontent in the country and fostered the protests. In Tunisia, in 2010, roughly a third of the population had access to the Internet, and half of those were on Facebook. Twitter was used only modestly by 0.34% of the population and thus played no major role in the revolution. This was mainly because Twitter, YouTube, and many blogs were blocked and could not be used. But Ben Ali had to keep the access to Facebook open because of protests, even within his own camp. The event that triggered the protests was the self-immolation by burning of Bouazizi in December 2010, but he was not the first to protest by way of suicide in Tunisia. However, the protests following his act in his home city were crushed by the police, and this was filmed. When it was broadcast via social networks and TV channels, protests were triggered in the whole country. The organization of these demonstrations was done mostly via social networks, which is why Ben Ali ordered the arrest of many Internet users shortly after the protests broke out and put pressure on people organizing protests. Party accounts were hacked by well-known regime critics to spread false information. The number of people using Facebook increased by 5% from the beginning of the protests until April 2011 from 17.5% to 22.5% (see Spiegel et al. 2013).

In general one can say that only Facebook had any measurable influence on the revolution in Tunisia. The importance of the Internet stems mostly from the publications of WikiLeaks, but the population was angry and discontent before because of limitations to freedom and high unemployment; thus the importance of these leaks should not be overestimated. The distribution of the video of the first protests was done mostly via social networks, but because these videos were broadcast on Al Jazeera "in every street café in Tunis" (cited after Spiegel et al. 2013), most people would have seen them anyway. The truly important thing was the organization of the protests. Even if cellphones and leaflets played an important role, Facebook allowed the mobilization of a quarter of the population within an instant. The protests were thus not triggered or enabled by social networks, but the organization was made much easier. Anyhow, people in Tunisia would have had many possibilities to protest and to organize protests even without social networks (see Spiegel et al. 2013).

The Role of Social Networks in Egypt

"When the demonstrations began in January 2011 there were 23.5 million people using the Internet. During the Revolution the number of internet users was increasing as well. In June 2011 there were already 25.9 million users" (cited after Spiegel et al. 2013). 25.9 million equals roughly 30% of the population. One and a half years before that, there were only about half this amount of people using the Internet.

Even before the demonstrations in the streets in January 2011, there were protests in the Internet against the regime and bloggers, who were engaged in human rights struggles and tried to explain how a democracy works and how a constitution is developed. For this blogs and increasingly Facebook were used. Basem Fathy, an Egyptian blogger, wrote that there were roughly 1500 bloggers. With Facebook and Twitter, the number of net activists rose to some 1.5 million (see Fathy 2011).

Basem Fathy describes the activity of net activists as being, at least in the beginning, unorganized and spontaneous. Only over the course of the revolution, the net activists explicitly tried to use Twitter as a news channel, for it had already proven to be helpful in Iran after the presidential election (see Ibid.).

"Even a deactivation of the internet did not hinder the use of social networks. After the internet was deactivated in Egypt, Telecomix net activists spread phone numbers via fax, with which one could log on to the internet via the phone cable and provided modem pools" (cited after Spiegel et al. 2013). Thus even after the deactivation of the Internet, a large part of the population was still active.

In Egypt mostly people from the upper and middle class have access to the Internet. The protests in the streets were however started by people from the lower classes. Only as time went by the middle classes joined the demonstrations. The Internet activists had no influence on the activists participating in the demonstrations (cited after Spiegel et al. 2013).

In Egypt social networks were used as the main source of information and education. The net activists had tried even before the demonstrations took the streets to inform the population about human rights and the advantages of a democracy.

The social networks were for sure not the reason for the outburst of the protests in Egypt. However, they could have contributed to the fact that large layers of the population took the street when the protests began. Additionally, more information was spread to foreign countries, which, without social networks, would have been made public only filtered or very slowly. Thus the international pressure on the regime rose rather quickly. Eventually, the activities in social networks led the demonstrations to success sooner (see Spiegel et al. 2013).

In general Facebook is used in the Arab world not only to keep in touch but also to mobilize people, be it for political, economical, or cultural issues. Facebook is also used to strengthen citizen journalism, as well as to improve the interaction between the government and the people (see Milz 2011).

If there is a great will to protest in the public, digital media are able to connect mobilized citizens quicker and more effectively and speed up or simplify the organization of protest, and especially through digital media, it is easier to spread the results of a given protest quicker and make them known to a wider public. It is

this last fact, the possibility of spreading information in a regional environment or on a global scale, which is of eminent importance and plays an important role, because this can put additional pressure on the autocratic rulers. In the Arab Spring, this transnational spreading has sparked a flame in the region (see, Ibid.).

Conclusion

No one is capable of predicting the future of the Arab revolutions. The events are still unfurling, the development will not be linear, and there are contradictions, triumphs, and defeats. These will entail frustration and desperation, similar to Ukraine or Georgia, where the promising beginning was crushed by incapable politicians. The Arab world is only at the beginning of an epochal change, which will carry on for decades and will occur differently in different countries. But one thing has already and unconditionally changed: consciousness. Newly gained freedom entails not having to wear a mask any longer. Before the revolutions even the children learned not to say what they thought. Now the era of old men in power comes to an end.

The biggest potential for a sustainable democratic change can be found in Tunisia and Egypt. In both countries there are functioning state institutions, a well-educated youth and middle classes as the carriers of social change, despite decades of interventions by authoritarian rulers. Both countries assume the function of role models. Is there a successful economic development in combination with a functioning and just law system and democracy, the other countries will orient themselves after them. Egypt is, after all, one of the leading powers in the community of Arab nations (Lüders 2011, p. 42f.).

Especially in Libya and Syria, in other countries of " Arab Spring," the perception of the "spring is not experiencing winter" has strengthened where the spread of democratization is unable to take concrete and lasting steps.

Egypt is seen as the most important countries of the Arab world. Claims that Egypt's democratization with the "Arab Spring" would make it possible to change in this direction in all areas and if this would not become real in Egypt, the "Arab Spring" would end (Traube 2011) are remarkable.

A heavy military coup in Egypt suffered a blow, and even the "Arab Spring" seems to come to an end. After military coup protests, the coup responded with weapons as a result to which thousands of people died. This act finished democratization hope; it heralds the demonstrations against Mubarak completely in the short term, and the instability and uncertainty judge has begun a process. If entered on a path toward democratization by Mubarak's ouster, it has ended as a result of the military impact (see Kocak 2014, p. 23).

The protests, uprisings, and revolts, even below the threshold of a regime change, already have a significant impact on the Arab domination systems. The scope for action of the regimes has considerably narrowed, and they are more dependent on the legitimacy of their policies than before. The measures taken so far are not sufficient in many places to end the protests and to sustain the domination systems

permanently. Therefore, the regimes will therefore not endure in their present form. In this respect, the Arab Spring is a historical caesura (see Asseburg 2016, p. 7).

Six years have passed since the mass protests in 2011, which led to changes in power in Tunisia, Egypt, and Libya and had further reactions in all countries of North Africa and the Middle East. The hopes of large parts of the population have been disappointed in the countries where power changes took place. The year 2011 was not the beginning of a policy change in any of these countries as it has not lead to more social justice, development in all parts of the country, state of law, and good governance (see Faath 2016, p. 11).

> *... Today many of the activists are in prison, old and new dictators are in power, millions of people had to face a civil war, hopelessness and the murderers of the so-called Islamic state. The Arab world is in a deep crisis that threatens to become a European one: hundreds of thousands of refugees, bloody terror attacks, diplomatic helplessness.* (See Gerlach 2016, p. 3)

Historical Outline of the "Arab Spring"

- December 17, 2010: The Tunisian vegetable merchant Mohamed Bouazizi burned himself.
- January 4, 2011: In Bouazizi's, more than 5000 people protested for better living conditions and against corruption in Tunisia.
- January 14, 2011: The Tunisian dictator Zine el-Abidine Ben Ali escaped to Saudi Arabia after 24 months**.**
- January 16, 2011: Ben Ali's escape motivated Egyptian demonstrators to protest against President (and dictator) Hosni Mubarak. In Tunisia, a transitional government was formed under Mohamed Ghannouchi.
- January 25, 2011: On the "Day of Wrath," thousands of Egyptians protested against Mubarak and occupied Tahrir Square in Cairo.
- February 1, 2011: By the impression of the protests, Mubarak announced that he would no longer run the government.
- February 11, 2011: Egyptian dictator Hosni Mubarak has not been in power anymore after 30 years.
- February 19, 2011: Libya's armed forces attacked rebellions in the country with massive weapons.
- February 20, 2011: Demonstrations in Rabat, Casablanca, and Marrakesh called for a new constitution for Morocco, but no end to the monarchy.
- February 27, 2011: The "National Transitional Council" of Libya was established.
- March 14, 2011: Saudi Arabia and other Gulf states sent units to Bahrain to support the regime.
- March 17, 2011: The United Nations imposed a flight ban on Libya.
- March 18, 2011: The assassination of two protesters in Deraa by Syrian government forces has caused nationwide demonstrations.

- May 7, 2011: Violence broken out between Christian and Muslim populations in Cairo. Nationwide protests against religiously motivated violence follow.
- June 3, 2011: The Yemeni dictator Ali Abdullah Saleh was injured by a bomb attack on his palace and went for the medical treatment to Saudi Arabia.
- August 3, 2011: The trial against Hosni Mubarak began in Cairo.
- August 21, 2011: Tripoli captured by Libyan rebels.
- October 20, 2011: The submerged Libyan dictator Muammar al-Gaddafi was killed in Sirte.
- October 23, 2011: The first free elections in Tunisia took place.
- November 16, 2011: Syria's membership in the Arab League was suspended because of violence against its own population.
- November 19, 2011: Gaddafi's fugitive son, Saif al-Islam, was arrested in southern Libya.
- November 22, 2011: The drafting Council of Tunisia met for the first time.
- November 28, 2011: The first round of the Egyptian parliamentary elections began.
- December 12, 2011: Moncef Marzouki was elected as President of Tunisia.
- May 31, 2012: The exceptional situation in Egypt has been lifted for the first time since 1981.
- June 2, 2012: Mubarak sentenced to life imprisonment.
- June 18, 2012: The still ruling military council in Egypt limited the powers of the presidency.
- June 30, 2012: Member of the Muslim Brotherhood, Mohamed Morsi, sworn in as president of Egypt.
- July 9, 2012: The Moroccan rapper Mouad Belghouat, who was sentenced due to a corruption song in the police, started a hunger strike.
- August 2, 2012: Because of the ongoing violence in Syria, Kofi Annan took the role as a mediator between the government and the resistance movement (see, Forum Politische Bildung 2012, p. 32).
- November 29, 2012: New constitution on the "principles of Sharia" in Egypt once again led to demonstrations, which ended with a military coup. The military Adli Mansur, a former official of Mubarek, was appointed as the president commissioner until the new election in May 2014.
- May 27, 2014: Abdel Fattah el-Sisi was elected as president.
- The Syrian Civil War, which has been still continuing.

The Process of Democratization of the "New" Turkey

The birth of a "new" Turkey is commonly associated with the election of the AKP to power in 2002. Since then Turkish politics is dominated by the moderate Islamic Party for Justice and Development (AKP) of Prime Minister Recep Tayyip Erdoğan. The AKP could extend its sole reign after the parliamentary elections of 2011. Even though it suffered a small loss in votes, it still has 327 of 550 seats and thus a

comfortable majority, which solidified its position as the first not entirely secular ruling party in the history of modern Turkey (see Schimm 2013).

Prime Minister Erdoğan is the decisive personality in Turkish politics. The AKP's electoral triumphs and a large part of its popularity are due to its leader, and without him the party would very likely suffer a huge drop in votes (see Schimm 2013).

The parliamentary faction of the AKP could initiate a process of reforms with its clear majority that eventually led to the beginning of the talks between Turkey and the EU with the goal of an eventual EU membership of the Turkish Republic. Roughly at the same time, the then foreign minister and now president Abdullah Gül opened NATO reform talks in Istanbul and urged in a speech in front of representatives of the OIC member states in Tehran for a necessity of democratic reforms in Islamic countries and to allow a contribution of civil society in the process of modernizing these countries (see Gül 2004).

The AKP government supports the economic, infrastructural, and industrial development of the country through a liberal economic and financial policy and opened Turkey for foreign investors. This allowed Turkey to acquire new markets for the increasing number of Turkish entrepreneurs. Since the year 2002, the GDP/capita in Turkey rose decisively, the Turkish Lira gained strength through a monetary reform, and inflation could be kept under 10% constantly. Because of the ongoing economic growth as a consequence of an increased consumption of the population and the relatively good situation of Turkish businesses, the Turkish economy made it through the global economic and financial crisis beginning in 2008 without major losses and instabilities, even though the debt of the state is still high and the social and economic differences are huge. The symbol of the "new" Turkey is Istanbul, with its hundreds of years of history and its diverse and cosmopolitan character, which not only attracts tourists and investors but also state officials from all over the world (see Schulz 2011).

To draw a first conclusion of these developments is however still difficult; for there are many problems still unsolved: Neither is the transformation of the state and the new constitution in a civil, democratic spirit finished nor are human and civil rights properly strengthened; the economic order stabilized in a sustainable way; the social, ethnic, and religious tensions in society resolved; the relations to all neighboring countries normalized; and the acceptance of Turkey to the EU secured. Nonetheless it has to be said that the AKP government has achieved many things and performed really well with their politics informed by the goal to change the country for the better, to protect it from the negative effects of globalization, and to prepare it for the twenty-first century (see Schulz 2011).

The government had planned to have a new constitution ready and signed by the end of 2012. This new constitution should contain more democratic elements and improvements regarding human rights and free speech. The effective constitution so far was still the constitution issued in 1982 as a consequence of the military coup d'etat and constituted one of the main points of criticism of the EU in the context of the talks over the accession of Turkey to the EU. Since the elections of 2011, the AKP has no longer the two-thirds majority necessary for constitutional changes, which means that it needs the partial agreement of the opposition (see Schimm 2013).

Is Turkey a Role Model for the Arabic Reform Countries?

There is no other country mentioned as often as a potential role model in the process of political transformation in the Arab world as Turkey. What is mostly emphasized are the similarities of Islamic culture, to which the democratization of Turkey is added. Turkey thus becomes the proof of a potential compatibility of Islam and democracy and is supposed to serve as a model for the Arabic countries in this regard. In the same vein the ruling AKP of Prime Minister Recep Tayyip Erdoğan serves as the model for the democracy-oriented "moderate" Islamists in the Arab reform countries. If such a simplifying reductive view of reality together with wishful thinking is the right approach for the complex relations in the region is highly doubtful. It is much more important to understand the specific path of development of Turkey, and the "new" Turkey has to be held accountable to further consequently pursue its path of modernization and democratization.

The message sent by Turkey to the countries of the Middle East in 2011 was clear (see Erdogan 9/14/2011a): first, Islam is not an obstacle to democracy and socio-economic modernization in the region. Rather, the authoritarian regimes, supported by the military, are the forces that really block social development. Secondly, all the countries in the region have the right to choose their own path to freedom and modernity, as long as they respect the republican and democratic framework, hold free elections, give themselves a free and democratic order of society by general consensus, and open themselves for political, economical, and social interaction and regional and global interdependence with other countries. Even if the leading Turkish politicians do not acknowledge it, they, as many spectators within and outside of the country, do regard Turkey as a model for the countries willing to transform themselves, as long as true assurance of democratic reforms, the willingness to negotiate and make compromises within the basic structure of a given system, and the integration of all layers and groups of society in a process of reconciliation and transformation are guaranteed.

But it has to be said that such positions are characterized by a large portion of wishful thinking and only make sense if one's perception of reality is considerably marred. The Muslim Brotherhood, for example, in its immediate response to Erdoğan's laicism recommendation, pointed toward the different path of development that Egypt had in the past compared to Turkey, which makes a strict separation of state and religion an almost impossible task to accomplish (see Erdogan, *Egypt's Muslim Brotherhood Criticizes Erdogan's Call for a Secular State*, 14.09.2011b). Furthermore, Egypt and Tunisia are only at the beginning of a very difficult process of transformation and democratization, a part of which is the subordination of military violence to a democratically elected civil government. However the further transformation of the "Arab Spring" countries will look like (see Orient-Institut 2011), it has to be stated that Turkey constitutes a fascinating phenomenon for many observers, because of decades-long cooperative relationship with the West and the new role Turkey plays for the Near and Middle East, which the "post-Islamist" AKP tries to write since 2001.

Thus Turkey assumes a model character, because the internal political process of growing toward republicanism and democratization, which has been continuing for

decades, occasionally set back and manipulated by military coups and a deficient civil political culture. Most importantly, what constitutes the specificity in the region is the institutional integration of Turkey into the Western community, be that as a NATO member or as a member of other international European organizations (Council of Europe, OSCE) – even though the question has to be asked to what extent, it was this integration that prevented Turkey from taking a similar development like the Arabic states, namely, toward systems that are authoritarian and dominated by the army (see Schulz 2011).

Current Political Position of Turkey

Today, Turkey is directed by Prime Minister Ahmet Davutoğlu on paper; however the actual head of state is Recep Tayyip Erdoğan. Since the elections of 2002, AKP holds the control of 312 seats of 550 seats at the parliament by keeping the majority and the power of constituting the government with a single party in the Grand National Assembly of Turkey. AKP was constituted in the year 2001. The party introduced itself as the defender of a Western orientation, a conservative society and a liberal economy. Western powers gladly welcomed the rise of this new party, with the thought of having a political platform which would bring well-managed democracy and Islam together under the governance of AKP. Also, Western countries did not want to have a too great distance from the powerful and strategic geopolitical location of Turkey. *In the last years*, *however*, *AKP is more intervening across the economic and social matters*. *Among all the other problems*, *they performed in a traditional manner on the issues such as the role of women and family*, *religious education*, *and alcohol consumption*.

In Turkey, where presidents stay out of politics traditionally, Erdoğan resigned from his party by achieving the victory of becoming the first president of the country, who was elected by society. This victory was the outcome of the change of the presidential election in 2007, which was approved with a constitutional referendum.

The former Foreign Affairs Minister Davutoğlu became the new Erdoğan as the Prime Minister and in the AKP. Erdoğan always played an important role in Turkish politics. The president mentioned the creating of a "New Turkey" and stated that he will continue serving for his country until the 100th year of the foundation of the Turkish Republic, 2023.

Moreover, he attempts to centralize the political power in his presidency. To make that happen, he aims to create an administrative model, which possibly can end the division of power in Turkey (see Ellis 2015, pp. 7–8).

Freedom of Press

The problems of the freedom of press in Turkey are factors of the history, legal traditions, and the current economic situation of the country. Throughout history, Turkey faced many threats of freedom of press, mostly under the governance of the government after a military strike. The primary threat is the rising authority of the AKP. Although the hopes of the protection of democracy and the hopes of getting

closer with Europe, the division of power has been weakened. Moreover, the party (AKP) has grown distanced with the European Union. As a result, the freedom of press has weakened even more.

The results of the share of unwanted ideas and information were heavy. Journalists and media channels, which did not pay any attention to the red lines, had to face consequences. Red lines were ideas such as accusation about the government or AKP's misuse of their duties.

Recent history shows that politicians, who govern Turkey, consider the media as a threat that must be controlled, not the guardian of the democracy. The actions can be mentioned in three points:

1. The politicians have some active efforts about the economic force in order to turn the media to their advantage.
2. Bad political environment gains power by taking attention with their narrow-minded and negative statements about the media.
3. There is a manipulation in judiciary and legal perspectives of the country.

This impact unites with the availability to get and share information online and also efforts for not being accused of the offenses against journalists, gaining strength under the control of the government (see Ellis 2015, p. 20).

In the last 7 years, Erdoğan has represented the political environment in Turkey with intolerant manners in the first place. The president always acts straightforward about his displeased thoughts against his political competitors, all opponents, and also judges of the constitutional court. In this manner, he does not stop talking negatively and in a damaging way, although he condemns the writings against the media. He prefers to do the talking in open sessions with the society (see Ellis 2015, p. 23).

In many cases, reasons for prohibition of a publication have been explained in reference to national security and the confidentiality of investigations. But observers state that, when the other tools do not work out, a reasoning would be applied as an excuse to prevent the share of information used to humiliate the authorities (see Ellis 2015, p. 29).

Government Repression of the Freedom of Expression on the Internet

In several cases, media could circumvent moves of information control attempted by the government. As a result, there is an even increasing pressure on traditional media, and a significant proportion of the dissident journalism in Turkey has migrated to online media.

Many people now think that Internet, online publications, and social media sites are the last remaining space for free expression in Turkey.

In consequence for this, in recent years, the government supporters redoubled their efforts to block access to websites and mobilized to respond to dissenting voices and the control of online content on the Internet (see Ellis 2015, p. 31).

Beyond any doubt, Erdoğan wanted to make the Internet legitimate under a greater government control.

Conclusion

Only gradually the "new" Turkey is getting rid of relics of the old times. The political powers and institutions keep on struggling against each other for resources of power and areas of competence, while neglecting the interests of the citizens. The parties still are lacking internal democracy and a liberal debate culture.

The Arab countries, longing for change and modernization, are however closely eying Turkey's steps toward a more liberal, pluralistic society within a democratic state, which acts responsible, and in a stabilizing way internationally. It should not be about prejudice and ressentiment, but the aim should be the whole: a sustainable and permanent stabilization of the region and a solution of the many conflicts in Turkey and its neighboring states (see Schulz 2011).

Turkey, on the paper, continues to be a democracy. However, the authorities fail on information sharing and the knowledge to protect human rights, and they take steps to undermine these rights in certain circumstances. All of this has led Turkey to a serious lack of democracy, and there are risks for the future of democracy (see Ellis 2015, p. 34).

The dismissal of Davutoğlu, the neo-Ottoman foreign policy architect, as prime minister in May 2016, can be seen as a clear sign of a realignment of Turkish foreign policy. Erdoğan's apology for the shooting of the Russian military jet and the resumption to Israel in accordance with the conditions of Israel are clear signs of a desire for normalization of Turkey's relations with its neighbors. Furthermore, the failed coup attempt by the Gülenist fraction on July 15, 2016 has been seen as a power struggle between the AKP and the Gülenist fraction in recent time. All of these situations could lead the AKP either to abandon the offensive orientation of foreign policy or to take an even more challenging position with a new set of miscalculations. Both options are characterized by an open outcome. Lastly, it can be concluded that the neo-Ottoman policy of the AKP in Syria and the Middle East has no future (see Türkes 2016, p. 109).

References

Ahl, A. E. (2011). Die Revolution zuerst. *DIE WELT*, 7.

Asseburg, M. (2016). Die Historische Zäsur des Arabischen Frühlings in "Dossier: Arabische Frühling"; Bundeszentrale für Politische Bildung, erstellt am 3.6.2016; bpb.de. Letzte Zugriff am 402.2017 / The historical caesure of the Arab Spring in: "Dossier: The Arab Spring"; Federal Agency for Civic Education, created on 3.6.2016; bpb.de. https://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi7zbz2hKfSAhUJtBQKHXWUAOQQFggaMAA&url=http%3A%2F%2Fwww.bpb.de%2Fsystem%2Ffiles%2Fpdf_pdflib%2Fpdflib-52388.pdf&usg=AFQjCNEuQGm_VARqIOap6V0_JOyPvQxZ2Q&bvm=bv.147448319,d.bGs. Accessed 12 Feb 2017.

Croiteru, J. (2011, May 21). Ägyptens Muslime werben im Christen (die Beschreibung der Parteiverfassung). *FAZ*, S. 35.

Cynthia, F. (2011, March 18). The Arab Upheaval: Egypt's Islamist Shadow. *Von The Middle East Quarterly, 18*(3), Summer 2011, S. 35. www.meforum.org/2887/arab-upheaval-egypt-islamist abgerufen

Ehrhardt, C. (2011, June 09). Aktivismus in Zeiten der Verunsicherung. *FAZ*, S. 1.

El-Gawhary, K. (2011). *Tagebuch der arabischen Revolution*. Wien: Kremayr & Scheriau.

Ellis, S. M. Democracy is under risk, International Media Institute Turkish special report, 2015: (IPI Savunu ve Iletisim Direktörü), Demokrasi Risk Altinda, IPI (Uluslararasi Basin Enstitüsü) Türkiye Özel Raporu. http://www.freemedia.at/fileadmin/resources/application/IPI_OEzel_Raporu_-_Tuerkiye_2015.pdf

Erdogan, R. T. (2011a, September 14). "Turkey's Erdogan tells Arabs to embrace democracy". *vor der Arabischen Liga und der Generalversammlung der Vereinten Nationen.* Vereinigten Nationen: defenceWeb. http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=19021&catid=74&Itemid=30

Erdogan, R. T. (2011b, September 14). *Egypt's Muslim Brotherhood criticizes Erdogan's call for a secular state*. Ägypten: News, Al Arabiya. www.alarabiya.net/articles/2011/09/14/166814.html

Faath, S. (Hrsg.). (2016). Nordafrikas Säkulare Zivilgesellschaften: Konrad Adenauer Stiftung e.V., Sankt Augustin, Berlin: letzte Zugriff am 16.02.2017 / North Africa's secular civilizations: Konrad Adenauer Foundation, registered association, Sankt Augustin, Berlin. http://www.kas.de/wf/doc/kas_47223-544-1-30.pdf. Accessed 16 Feb 2017.

Fathy, B. (2011, September 19–30). *Facebook Revolutionen? – Die Bedeutung von Social Media für den politischen Wandel in der arabischen Welt.* Abgerufen am 14. 08 2013 von Politische Bildung online: virtuelle-akademie.de. http://politik-digital.de/wpcontent/uploads/transkript_basem_fathy.pdf

Forum Politische Bildung. (Hrsg.). (2012). Timeline Arabischer Frühling: in "Medien und Politik"; Informationen zur Politischen Bildung, Bd. 35; Innsbruck-Wien-Bozen: Studien-Verlag. Letzte Zugriff am 24.02.2017 / Forum Political Education: Timeline Arab Spring in: "Media and politics"; Information on Political Education, Bd. 35; Innsbruck-Wien-Bozen: Studien- publishing company. http://www.politischebildung.com/pdfs/35gesamt.pdf. Accessed 24 Feb 2017.

Gerlach, J. (2011, June 17). *Ägypten: Wie stark sind die Muslimbrüder?*. Abgerufen am 17. 8 2011 von ZDF heute. www.heute.de/ZDFheute/inhalt/30/0,3672,8245630,00.html

Gerlach, J. (2016). Was ist schief galufen- in Ägypten, Syrien, Libyen. . .?, Der verpasste Frühling; in "Politik und Zeitgeschichte"; Ch. Links Verlag Frühjahr 2016.Letzte Zugriff am 22.02.2017 / What went wrong- in Egypt, Syria, Libya . . .?, The missed spring; In "Politics and Contemporary History"; Ch. Links publishing company spring 2016. http://www.christoph-links-verlag.de/pdf/vorschau_f2016.pdf. Accessed 22 Feb 2017.

Ghannouchi, R. (2011, February 16). Jeder soll entscheiden, was er trägt. *FAZ*, S. 6.

Gül, A. (2004). Turkey's role in a changing Middle East environment. *Middle East Quarterly, 15*, 1–7.

Jelloun, T. B. (2011). *Arabischer Frühling: Vom Wiedererlangen der arabischen Würde*. Berlin: Berlin Verlag.

Kneuer, M., & Demmelhuber, T. (2012). *ldung Bd. 35, Innsbruck-Wien-Bozen.* Abgerufen am 12. 08 2013 von Die Bedeutung Neuer Medien für die Demokratieentwicklung. http://www.politischebildung.com/pdfs/35kneuer.pdf

Kocak, K.-A. (2014). Legislation specialist, the speakership of the Turkish Parliament, International Relations Department, Egypt: one step forward two steps backwards on the way to the democratization. *Legislation Magazine* 23. http://www.yasader.org/web/yasama_dergisi/2013/sayi23/5-53.pdf. Accessed 8 Sept 2015.

Kreft, H. (2011, September 21). *Bundezentrale für Politische Bildung*. Abgerufen am 05. 01 2013 von http://www.bpb.de/apuz/33126/die-arabische-welt-braucht-mehr-jobs-mehr-bildung-und-mehr-demokratie-essay

Lüders, M. (2011). *Tage des Zorns*. München: C.H. Beck oHG.

Mainz, E. H. (2012, February 02). Abgerufen am 04. 01 2013 von Konrad Adenauer Stiftung. http://www.kas.de/wf/doc/kas_30185-1522-1-30.pdf

Milz, K. (2011, July). *Konrad-Adenauer-Stiftung e.V.* Abgerufen am 13. 08 2013 von Die Bedeutung Sozialer Netzwerke in der arabischen Welt. http://www.kas.de/wf/doc/kas_23306-1522-1-30.pdf

Orient-Instituts, S. d. (2011). *Ursachen und Entwicklungstrends der Veränderungsprozesse in den Ländern des Nahen und Mittleren Osten.* Abgerufen am 07. 08 2013 von Der Arabische Frühling. Auslöser, Verlauf, Ausblick. www.deutsches-orient-institut.de

Pott, M. (2012). *Der Kampf um die arabische Seele*. Köln: Kiepenheuer & Witsch.
Preiss, B. (2012). *Zeitenwende im Arabischen Raum*. Wien: LIT Verlag.
Schimm, M. (2013, March). *Länderanalyse Türkei.* Abgerufen am 11. 08 2013 von Bayern LB (Bayerische Landesbank). http://www.bayernlb.com/internet/media/internet_4/de_1/downloads_5/0100_corporatecenter_8/5700_volkswirtschaft_research_2/laender_1/laenderanalysenl_z_1/tuerkei_1/Tuerkei.pdf
Schulz, L. (2011, November 02). *Network Turkey discussion paper No. 8.* Abgerufen am 11. 08 2013 von Die neue Türkei: Vorbild für die arabischen Reformländer? http://edoc.bibliothek.uni-halle.de/servlets/MCRFileNodeServlet/HALCoRe_derivate_00005548/NT_Discussion_Paper_No8.pdf;jsessionid=A91D9E014F40954CBB53C29F7661B078
Sharp, G. (2010). *From dictatorship to democracy. A conceptual framework for liberation* (4th U.S. Ed.). East Boston: Albert Einstein Institution.
Spiegel, F., Rosenberger, P., & Wartke, E. (2013). *PhiloTec: http://et.fh-duesseldorf.de/home/philotec/philotec.htm*. Abgerufen am 12. 08 2013 von Die Rolle sozialer Netzwerke bei der Demokratisierung. http://et.fh-duesseldorf.de/home/philotec/data/spiegel-ua-social-media-demokratie.pdf
Teorell, J. (2010). *Determinats of democratization. Explaining regime change in the world.1972–2006*. Cambridge: Cambridge University Press.
Todd, E. (2011). *Frei! Der arabische Frühling und was er für die Welt bedeutet*. München: Piper Verlag.
Türkeş, M. (2016, March). Die Außenpolitik der türkischen AKP im Nahen Osten vor und nach dem "arabischen Frühling" in "Die Außenpolitik der türkischen AKP im Nahen Osten"; Zeitschrift 'Kurswechsel' 3/2016: 103–109: kurswechsel.at. Letzte Zugriff am 23.02.2017 / The foreign policy of the Turkish AKP in the Middle East before and after the "arap spring" in "The foreign policy of the Turkish AKP in the Middle East"; Magazine 'Kurswechsel' 03/2016: Pages 103–109: kurswechsel.at. http://www.beigewum.at/wp-content/uploads/KuWe316KW_Mustafa-T%C3%BCrkes.pdf. Accessed 24 Feb 2017.
Windfuhr, V. (2011, June 26). *Nach der Revolution: Ägypten erfindet sich neu.* Abgerufen am 17. 8 2011 von Spiegel Online. www.spiegel.de/politik/ausland/0,1518,770374,00.html

Transformation Toward Cyber-Democracy: A Study on Contemporary Policies, Practices, and Adoption Challenges for Pakistan

33

Shahzad Memon and Jawad Hussain Awan

Contents

S. Memon (✉)
University of Sindh, Allama I.I.Kazi Campus, Jamshoro, Sindh, Pakistan
e-mail: Shahzad.memon@usindh.edu.pk

J. H. Awan
Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan
e-mail: jawad.awan@scholars.usindh.edu.pk

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_50

Abstract

Cyberspace and its services are playing a vital role in this modern world because of their capacity to transform traditional or everyday working systems into cyber services. e-commerce, virtual learning, and eHealth services are some cases which are adopted globally to facilitate investors and consumers to monitor and interact all the time and allow provision of education and efficient health services for citizens. Pakistan has a population of 182.1 million, and youth under the age of 25 constitutes 63% of the total population. From this young community, more than 80% are active Internet and smart technology users, and the majority of them are "netzians." The youth segment has the power to move the country into the next phase of political and economic independence if it can effectually mobilize. Many of them are working as young leaders and actively involved in activism in politics, human rights, labor rights, media, and science and technology. All these fields are important to strengthen the governmental democratic norms of the country, and interaction between these young leaders will lead to develop a core of democracy and its norms. In a democratic setup, elections play a central role in stability and development. However; the real challenges are to ensure that the election processes are free, fair, credible, and transparent. The result of transparent elections is to reduce the risks of conflict and in fact lead to democracy, stability, peace, and development. From previous experience of elections in Pakistan, it seems clear that this all-important transparency and fairness in electoral system can only be made possible through effective usage of cyberspace and smart technologies. It seems that young people in Pakistan can easily accept cyber democratic processes. However the transformation toward cyber democracy will have many challenges such as political resistance, public acceptance, cultural barriers, awareness and availability of smart technologies, and load management on communication networks. This chapter will discuss contemporary government policies, practices, and strategies for the transformation of traditional democratic processes into cyber democracy. In addition, this chapter will focus on the critical review of cyber bills and policies, theoretical and empirical frameworks, technological challenges, cyber democracy research models, and future strategies in the development, implementation (including overcoming barriers), and acceptance of cyber democracy in Pakistan.

Keywords

Transformation · Democracy · e-voting · Cyber democracy · Pakistan · Cyberspace · e-governance · Cyber-crimes · Practices and policies

Introduction

Our emerging digital world demands change or revolution, each of which can have either a pessimistic or optimistic impact. This evokes the famous saying that "change or transformation practices come collectively with foremost challenges" (Hénard and Roseveare 2012). A diversity of aspects is causative and liable to driver

evolutionary practices. In our perspective, a worldwide network setup and a worldwide communication system are the most serious issues. Furthermore, the increasing availability of a worldwide network setup and communication system is intimately associated and fabricated on innovative developments in the domain of ICT.

"Will cyber democracy be the future of Pakistan?" Usually new scenarios have been highlighted from the virtual world, which can be in the form of cyber fraud or cyber-crime or cyber harassment or malware. At this time developing countries are also the target of cyber-criminals/activists because of implementation and deployment of new technologies. Because of the regulation and surveillance of people that are associated with cyber systems, cyber democracy as an upcoming product for Pakistan holds huge democratic uncertainties. Nowadays, it appears nearly unfeasible to make a reality all the desirable protection stages that cyber democracy entails for involvement, struggle, liberty, and fairness in the virtual world. From the collected information, it seems that a cyber democracy requires a higher level of security and policy to be the future of democratic society. This is despite the fact that cyber democracy would be an incredibly functional tool to communicate with citizens as well as for government to share information and offer government services. Cyber democracy connects a nation to be part of a democratic practice throughout different channels that currently exist in the age of the digital world. This active practice will be more attractive to perceive if revolutionary change could not be effected by the political or virtual world in Pakistan. Middle East will be intensely impacted because of cyber democracy in future (Abbott 2012).

The analysis, which is being presented here, is structured in nine sections. After the introduction section, "Cyberspace" discusses cyberspace; section "e-government Services" demonstrates e-government services, factors, and their solutions; section "e-governance" refers to e-governance and risk factors within the implementation process; section "e-voting" discusses e-voting and its implementation; section "Democracy in Pakistan" reflects on democracy, its status, and failure causes in Pakistan; section "Cyber Democracy" discusses cyber democracy and its objectives; section "Transformation of Democracy" highlights the transformation of a democracy; finally, in the closing of the final section, section "Conclusion", a summary is being developed about the effects of transformation of democracy to cyber democracy in Pakistan.

Cyberspace

Cyberspace is a global field of information environment, which is one of the foremost inter-reliant fields (air, land, maritime, and space are the remaining fields). Cyber operations rely on IT infrastructures of an inter-reliant network comprised of the Internet, computer networks, digital systems, embedded microprocessors, and system controllers (Awan et al. 2017), as well as means of monitoring the flow of content among these components. According to the Secretary of Defense Robert Gates (Staff and Operations n.d.), cyberspace and its linked tools offer exceptional chances to the USA which are essential to national security as well as entire phases of

military operations. Cyber operations rely on associations and nodes that exist in the physical domains and execute tasks practiced either in cyberspace or physical domains. For instance, in cyberspace actions can facilitate sovereignty of action for physical domain actions. These physical domain actions can produce possessions via cyberspace by disturbing the EMS (electromagnetic spectrum). The association between cyberspace and space is distinctive as well, since space operations are a significant segment of cyberspace and depend on cyberspace services via space operations. Space fields are providing an important worldwide connectivity selection for space operations (Kaczmarczyk 2011).

e-government Services

According to Backus (Palvia and Sharma 2007), (Awan and Memon 2016), there are three essential target groups those can be easily connected: business, government, and citizen. Furthermore, two strategic objectives have been proposed. One strategic objective is known as external strategic which focuses on citizens and businesses groups, and the other one is internal objective which focuses on government only. In addition, Government to Government (G2G), Government to Business (G2B) or Business-to-Government (B2G), and Government to Citizen (G2C) are essential services for a government to offer their public which has been discussed below:

G2C

G2C is an interactive platform designed for citizens, which offers a huge number of informative and relevant information to the citizen which can be easily accessible online via the Internet. These types of platforms or applications facilitate citizens to know governmental practices as well as ask queries regarding government agencies such as filing income taxes, paying income or real estate taxes, renewing driver's licenses, paying traffic tickets, and getting their response quickly as well as providing useful suggestions.

G2B

G2B is an activity which is associated with government and business organizations: the government pacts with commerce groups and suppliers about their services and products. G2B is responsible for two bidirectional interactions and transactions – either G2B or B2G. In B2G, business products and services are sold to government while in G2B governmental products and services are sold to business groups such as suppliers. Moreover, e-procurement service has been introduced, which is currently the key domain of government or business firms. In this way, auctioning of government surpluses and e-procurement are two key areas of government. Government procures big number of MROs (Maintenance

Table 1 Aspects for e-government environment in developing countries

Aspects	Symptoms	Effects
Institutional limitations	Inadequate planning Uncertain scope	Poorly intended system having more expenditure cost
Human resources	Lack of skilled workforce Lack of trainings	Inadequate sustain Isolation of technology sources
Arrangements of financial support	Undervalue scheme costs Requires recurring costs	Ongoing scheme Maintenance expenditures
Environment	Lack of seller demonstration	Lack of experienced technical maintain
ICT changes	Need of back-up service for systems Partial hardware and software Inappropriate software programs	Implementation Issues System inappropriateness
Legal insufficiency	Complex lawmaking practice	More dependence on client appliance Lack of official framework

Repairs and Operations) services or products directly from suppliers. ESDS (Electronic Service Delivery Scheme), IGSD (Interactive Government Service Directory), and ETS (Electronic Tendering System) are some good examples of G2B services (Bill Phelps 2015).

G2G

G2G is an internal activity which is associated with internal practices of government which compacts with the behaviors of diverse government firms which can be acquired easily. A large number of activities are intended for civilizing the competence and efficiency of overall government procedures. Intel ink is an example of this activity which carries confidential information shared by various US intelligence bureaus. Furthermore, various aspects of e-government services have been defined in Table 1.

From the collected literature (Palvia and Sharma 2007), governments initiate with the delivery of information online, although people or customer order and domestic competence inquire for new composite facilities for customers. The delivery of services online and functionality of ICT tools, procedures, and techniques in government processes play an important role inserting single or multi aspects of firm, future democracy, and e-governance in following stages of e-government solution. The e-government solutions at every stage are illustrated in Table 2.

e-governance

e-governance is simply a government application available on the Internet. The purpose of e-governance is to sustain or abridge domination for every party such as citizens, businesses, and government. ICT tools connect each party and maintain

Table 2 e-government solutions

	G2C	G2B	G2G
Stage 1 information	Information about local, departmental, and national. Such as: Statements, structure of organization, addresses, record of employees, laws, policies, and regulations	Information of business such as: addresses, record of organization, laws, policies, and regulations	Static Intranet & LAN
Stage 2 interface	Downloading, submission, filling of online forms from websites. E-mail corresponding, discussion groups, notifications and more	Downloading, submission, filling of online forms from websites. E-mail corresponding, discussion groups, notifications and more	E-mail, interactive tools
Stage 3 renovation	Customized website with incorporated personal account for all services	Customized website with incorporated business account for all services	Integration of databases

procedures and activities. e-governance and good governance have similar objectives. However, good governance is utilization of economy and enables political and administrative authorities to handle interaction of a country, provinces, states, etc. (Basu 2004). e-governance provides interaction between government and citizens to perform operations which improve the aspects of governance such as democratic institutions, government and business.

Risk Factors While Implementing e-governance

Whenever, e-governance is implemented the following factors have to be examined and their solutions could be implemented.

- Stability of politics
- Sufficient authorized framework
- Reliance level in government
- The significance of government identity
- Economical structure
- Structure of government either centralized or decentralized
- Diverse stages of maturity
- Demand of Constituents.

Abovementioned factors are barriers of external e-governance and frequently concern collapsed or misplaced components or required flexibility in the extensive frameworks of government that facilitate e-governance. Adjust the e-environment and governments have to set up a legal framework that behaves electronic practices and conventional practices equally.

e-voting

e-voting (electronic voting) is an essential functionality inside the field of cyber democracy. Traditional voting practices are infamous on account of irregularities, poor management, and scams and lead often to losers calling and demanding for re-election or recounting of votes. Voting practices face an extensive variety of technical and public troubles that must be analytically tackled – from the registration and authentications of voters and then the casting of votes carried out. Then, the counting of votes takes place and, finally, results are going to be announced.

In the worst cases, such voting issues result because of political crisis, which happened in Ukraine in 2004 and 2000 in USA. Brazil is the first country which has fully computerized balloting in the year of 2000. 600,000 e-voting machinery were used effectively in 2004 elections in Indian state. e-voting machines used in India were designed and implemented by ECIBE (Electronics Corporation of India and Bharat Electronics). e-voting machinery operated by battery, which is convenient, simple to work, consistent, tamper-proof, and fault-free. The administrator is assigned the duty to monitor election procedure at nominated polling stations. Furthermore, uneducated and illiterate voters would be capable to vote by identifying pictures, sign of the nominee, or his/her party identity. This technique saved the counting time as well as reduces the expenses of ballot papers.

e-voting is the key tool to accomplish the third stage of its growth. Furthermore, technology and e-voting are relatively well advanced nowadays. Nearly 10 million people cast their vote electronically and nearly 0.5 million via Internet in the world.

The USA, Brazil, and India are the leading e-voting systems users. India and Brazil have introduced centralized e-voting by using tools designed for the government.

Democracy in Pakistan

Democracy can be considered as a natural political system. However, Pakistan has interchanged between democracy and military rule. Participatory political establishment and procedures did not sufficiently develop sturdy roots in society so as to be profitable. Furthermore, the democracy ranking defined Norway, Sweden, Finland, Denmark, and Switzerland are the top five scoring countries in the ranking of 2010, and Nordic countries are universal top positioning and impressive countries because of reproducing a stable elevated score in the diverse dimensions by scoring in knowledge, equality, and gender (Campbell et al. 2013).

Liberty, control, sustainable development, and equality are basic elements quality of democracy. Mostly sustainable development contributes a novel and modern democracy theory, which assists to evade that dimensional structures of democracy are partial toward a left or right-leaning ideological limit of political favoritism. Knowledge and novelty are important tools because of the development of cyber democracy which requires knowledge of society, economy, and democracy (Campbell et al. 2015).

Pakistan practiced episodic legitimate and political collapse, the ascent of military administration, and the usurpation of rule by the generals who interfered with the political system to maintain their dominance in the political system.

Pakistan's current democracy is endangered by poor governance in both federal and provincial governments, a decreasing economy, declining internal cohesion and unity, spiritual and literary intolerance, and terrorism.

Some elements are defined as under for the quality of democracy in Pakistan (Ahmed and Khwaja 2013):

1. A populous government with altruistic headship
2. A trustworthy, sovereign, and unbiased electioneering association and procedure
3. Tracheotomy of influence between administrative, courts, and parliament
4. Security of citizens
5. Feasible, operational organization of liability
6. Accurate to open education and essential health care for each citizen
7. Financial equality
8. Religious patience

Pakistan lies between India and Afghanistan, which are extremely sensitive neighbors in a tremendous tension-ridden physical situation. Thus, the examination does not imitate situation in Kashmir (administered by Pakistan) and Baluchistan state adjacent to Afghanistan.

The Status of Democracy in Pakistan

In this subsection, seven principles will be discussed to highlight the future of democracy in Pakistan, under the following heads (Inayatullah 1997):

- The democratic model requires political establishment as well as progressive struggle which are completely dependable upon the rule of law, also assuring human freedoms and rights.
- State and political establishment requires modification in structural stability.
- Political society is a political platform where the most pressing objects and ideological partitions are condensed on the basis of fairness.
- Democratic standards have been extended constantly, also ensuring and reinforcing associations between a democratic community and democratic polity.
- Democracy is a distinct which can be extended from political and civic grounds to economic grounds.
- Local democracy is the inspiration among the public and citizens which is helpful for their dominant cultural systems and which replicates religious, cultural, and epistemological promises.
- Freedom restrains releases? The improvement of democratic potential from the limitations of the rising world order.

Causes of Failure of Democracy in Pakistan

- Almost 70% the population of Pakistan is resident in rural areas and leading their lives in feudal and rural traditions. This leads to poor families and landless peasants voting for the land owners, out of insufficient knowledge or fear. Thus, powerful and leading persons are selected in general election.
- Literacy is the primary condition for democracy. Unfortunately, Pakistan has 56% literacy rate according to the report published in 2015 (Sekho 2016).
- An independent government has to provide integrity, common well-being, and protection to its citizens.
- Corruption and fraud are common trends as well as no concept about the security of citizens and people are being killed and targeted on the name of honor (Pak Institute of Peace Studies 2014). The ratio of suicide attacks is increasing day by day due to poverty and unemployment (Akhtar 2016).
- Some recommendations have been highlighted to make democracy a success in Pakistan as well as reinforce the integrity of the nation.
- Traditional practices such as inheriting of political positions should be abolished.
- Rural community and citizens should be given education and liberty.
- Social equality, integrity, and laws should be followed and implemented for the entire nation equally, and their practices should be monitored.
- Youth, new talent, energetic, literate people should be encouraged and promoted.
- Genuine and competent leadership will be formed when educated, literate, and energetic people are recruited.

A flourishing implementation of the abovementioned practical procedures can guide our country and lead toward genuine democratic practice. If new democratic practices will not implement then the same practices will be repeated as happened in the past (Gautam 2011). Furthermore, a number of factors have been highlighted which can decline the democracy of Pakistan (Inayatullah 1997):

- The position of the armed forces
- The lack of tolerance in civil society
- The incidence of bribery at structural levels
- The formation of political economy
- The political opinions and policies of parties
- Formative modifications in the nature of democracy
- The function of magistrates in corresponding to the subjective control of the state

Cyber Democracy

Cyber democracy is based on e-governance and focus on the procedures and novelty allowed by ICT, which are shared with upper rank of democratic incentive and intention. The concept of cyber democracy is selected by the European Council which cover up the utilization of digital ICT tools in the vicinity of open activity,

associations between the authorities of civil community and society, also the involvement of the these authorities at each stage of democratic practice, and the stipulation of public services (Directorate General 2016).

Cyber democracy is a democratic process in which online government activities, the elected legislature, political parties, and citizens play an important role. This includes biased or existing interaction symposium or consultation among legislature and their constituent. This cyber service has played a vital role in the 2004 election and 2006 midterm elections in the USA. All the parties' candidate had their personal e-portals and also communicates with potential voters via e-mail messages. This happens also in South Korea where politicians rely on Internet to recruit voters.

Cyber democracy involves e-engagement, e-consultation, and e-controllership. e-engagement engages the public in policy development via the Internet. e-consultation provides interaction between government employees and public and business groups, and online controllership includes the potential to supervise the expenditure, efficiency, and offered services of an organization electronically (Palvia and Sharma 2007). Cyber democracy is normally considered as a tool for discarding the representative system with the commitment of voter. To accomplish these objectives, government representatives are demanding to build up satisfactory e-government approaches that will decide to a greater level the accomplishment or collapse of the resulting e-government scheme. Cyber democracy has a well-known position in the e-Government literature. e-government is not only transforming governmental services (known as e-administration), it also transforms the political systems (known as cyber democracy). Cyber democracy has taken the benefit of technologies and the Internet, which helps citizens to insist on and acquire content while being online. ICT technology has enhanced the extent and excellence of community contribution in government and emphasizes the opportunity for direct democracy on a big scale.

Objectives of Cyber Democracy:

- Synchronization and accomplishment of policies as well as service deliverance online
- Designing and implementing programs for citizens
- Support and boost citizens for participation
- Ensuring online service deliverance by investigation and assessment as well as evaluate effectiveness and benchmarking of offered services
- Indexing of country

Implications of a Cyber Democracy in Pakistan

From various discussions, conferences and gathered literature about cyber democracy and its domain highlighted risks and future targets. Though, few implications have been discussed and illustrated in Fig. 1.

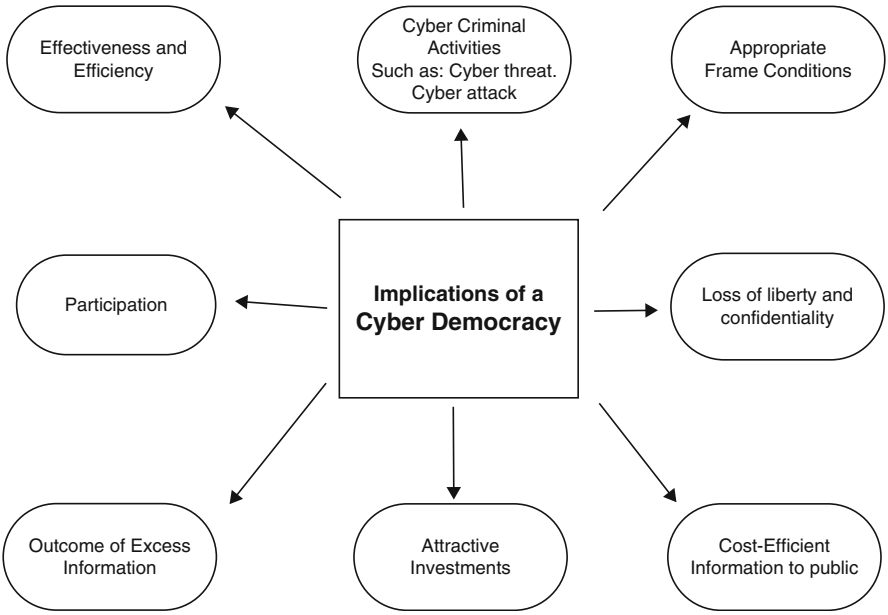


Fig. 1 Implications of cyber democracy in Pakistan

Conveying of Information to the Public

Cyber democracy allows modern techniques and channels for conveying appropriate information to the public. Furthermore, cyber democracy provides information to the public in a cost-efficient manner. With the help of the latest media, the public will be updated more quickly regarding democracy and interrelated administrative necessities. This type of information transformation will also be more comprehensive and much enhanced with an improved quality.

Attractive Investments

The latest digital and effective media have to be built up and executed by the states to guarantee well-updated citizens and public in a cyber democracy. The number of participants increases this results in greater democracy. In this way, cyber democracy emerges to be very difficult and have to be considered sustainably. So, this entails immense investments by the state eager to extend in this trend in addition to essential inventive success.

Outcome of Excess Information

It is possible that people may not differentiate appropriate and irrelevant information about democracy in the cyber democratic environment. In this regard, new innovative ideas and strategies are required to classify the democratic information society. Furthermore, interactive and attractive websites and blogs have to be developed to share and present information correctly. This approach will classify the democratic information society accordingly and displays full transparency for the public and citizens.

Participation

Cyber democracy provides more opportunities to the public as being part of new innovative technology as well as increasing their attention toward participation in the democratic practices and procedures which is supportive in their societal and political lives. Discussion forums, chat rooms, discussion blogs, and social sites are examples which depend on the Internet or the improvement of ingenious digital forms for the benefit of voting or view ballots. This type of discussion or activity could be performed daily or at scheduled times.

Effectiveness and Efficiency

Cyber democracy offers a wide range of services which require involvement in the digital world and existing technology of government. ICT tools and modern technology are the basic needs for public and government. Although citizens can ask queries and download and request information or applications easily via Internet, the government can take advantage of Internet to monitor and assess the role of citizens and offered services also. This approach will enhance the communication process and results in faster response between people and administration, providing an optional and supplementary duty of administration available outside working hours.

The Threat and Attack of Cyber-Crime

In the modern digital information age, technology is growing day by day, and introducing modern innovations and technology is also moving toward cyberspace and cloud computing which are based on Internet service or network connectivity. Thus, the attraction of cyber-criminals toward these services may increase and will target cyber democratic practices or its domains for their benefits, breaching security measures, as well as exploiting cyber democracy services or trying to reduce the participation of citizens (J H Awan et al. 2016). Cyber-criminal activities are complex to guard against. Smart cyber democratic awareness and solutions for security queries and problem resolutions must be identified as a matter of priority. Safety solutions for their implementation appear to be a significant requirement for the successful establishment of cyber democracy. How then to protect cyber democracy from cyber-criminal activities? This question may arise in the future. The ambiguity of the Internet should be appreciated, and participant identification must be ensured, verified, and be treated in the same way as happens in the non-virtual real world, to enable the citizen to dynamically join in a cyber democracy.

Cyber democracy requires professional and skilled personnel to keep secure the democratic system and public from virtual world. At present, various numbers of countries including Pakistan are really unsecure against cyber targets and attacks. Cyber democracy has to propose and design security frameworks to monitor and assess the performance of cyber democracy services and control the cyber attackers who have intelligent and modern sophisticated systems.

Appropriate Frame Conditions

It is vital role of democracy that politicians design policies and strategies with a view to creating a suitable and desirable environment. Proposals have to be given

preference which connect Pakistan with other countries of the world and enhance a stronger and more fruitful digital communication landscape. To bring about a cyber democratic system, central or regular communication networks and their connections have to be ensured, and some security practices must be implemented.

Loss of Liberty and Confidentiality

It is also difficult for the citizen to remove their data that are either collected or in the domain of the virtual world because each and every task is carried out by people in this virtual world via Internet.

Internet users have achieved and will continue to achieve enormous potential, and global communication has developed more easily, although digital users must be attentive about loss of liberty and confidentiality (Carayannis et al. 2014).

Transformation of Democracy

At the current stage, democratic societies are needed to transform, and few objectives are discussed and illustrated below:

1. Increasing the participation of civic society, e.g., by using additional traditional referendums for political choice
2. Additional improvement of the citizen's liberty and fundamental privileges
3. Additional social safety for the people by guarantee of livelong necessary profits
4. Additional firm and achievement of the information civilization
5. To develop sustainable and future proof environment by a Green New Deal on both the nationwide and supranational stage and in successive steps at an international level

Barriers of Implementation of Cyber Democracy in Pakistan

In the implementation process, various barriers can interrupt the advancement to comprehend the promise of e-government. The diversity and complexity of e-government schemes entail the reality of a number of barriers and challenges in the implementation process. This subsection highlights mainly significant and regular challenges and barriers which are mentioned as follows:

- Infrastructure of ICT tools
- Isolation and protection
- Code of conduct issues
- Need of experienced and trained personnel
- Need of firm and alliance
- Digital segregate
- Civilization
- Privileged and executive support

Transformation Challenges of Democracy to Cyber Democracy for Pakistan

In this section, 13 challenges have been discussed along with their recommendations for the transformation of democracy to cyber democracy for Pakistan (Basu 2004):

- The development and implementation of infrastructure
- Policies for public and law
- Digital segregate
- e-literacy
- Accessibility
- Reliance
- Privacy
- Security
- Transparency
- Interoperability
- Management of records
- Stable conservation and availability
- Marketing and education
- Public and private partnership
- Personnel problems
- Cost structures
- Benchmarking

The Development and Implementation of Infrastructure

- Propose and design projects which shall be compatible with telecommunication.
- Deploy kiosks and mobile centers for public access (When tele compactness is low).
- Accelerate the deployment of digital technologies by introducing telecom workshops, competitions, and conferences.
- Ensure the sustainability to build and bring connectivity to underserved areas on the microenterprise.
- Launch a compatible structure at the start of the practice to permit for a rational and synchronized asset endeavor down the road.

Policies for Public and Law

- Consult with stakeholders to review the execution of existing laws which hinder the preferred results.
- Provide authorized status of online published information.
- Elucidate the regulations and rules and permit filing electronically.
- Simplify the regulations and procedures for the development processes.

Digital Segregate

- Offer shared or mutual access via central computers.
- Schedule training opportunities.
- Motivate and encourage private sectors as they contribute and participate in government scheduled trainings.
- Highlight the adopted local language and content.
- Employ entrepreneurs to establish and sustain access points in societies, remote areas, and communities.

e-literacy

- Guarantee the content which is in local languages and its interface is simple to use.
- Utilize multimedia such as speech or pictures in new developed applications.
- Deploy learning modules in e-government projects.
- Offer workshops and trainings to the citizens for the improvement of basic computer skills.
- Establish various training programs about e-government.
- Organize seminars for the awareness of women, elderly, and immigrants.

Accessibility

- Design modern applications for disabled persons, such as an audio or visual.
- The government adopts the new merging technological tools to support the disabled person.
- Schedule and set criteria to measure efficiency and advancement.

Transparency

- Publish laws, rules, and necessities for government services online to reduce personal trials by representatives.
- Senior and skilled professional authorized can accelerate precision and liability efforts by redesigning offices structure as optimistic model of sincerity.
- Train the citizens via online trainings as they monitor and track the status of applications online.
- Train and motivate civil servants for development.
- Incorporate transparency and practice transformation to simplify rules and measures.

Interoperability

- Plot and review accessible record system.
- Recognize and change rigid systems, those building communication with the government onerous.
- Apply regular principles during the government, to reduce the progress period and guarantee compatibility.
- Implement a government approved IT infrastructure.

Record Management

- Enhance data sharing techniques.
- Increases cooperation among governmental institutes and community.
- Computerize the records which can be easily published online and easily maintained in record keeping.
- Creation and standardization of metadata is important in record keeping to conduct successful data search.

Secure Conservation and Accessibility

- Propose and develop applications as per requirement.
- Consider significance, usability, compatibility, and affordability of language.
- Sustain cooperation between government institutes and community in gathering, storing, and utilizing information, although progress constantly with individually particular information.

Marketing and Education

- Enhance advertisement and training activities that will connect and share e-government information within the community and enterprise.
- Accomplish research centers to ensure Internet services, which are giving a proper response according to needs and the implementation is suitable for the objectives of audience.

Public and Private Firm

- Create multi-sectoral firm.
- Evaluate and reexamine rules and strategies of those obstructing public/private collaboration.
- Make sure that contract with contractor and associate is reasonable and can be assessed and improved over time.
- Request support and participation from organization that previously have practice in offering services and information via technologies.

Personnel Problems

- Plan a time frame for accomplishment in a systematic manner, thus the development will not appear irresistible to the administration.
- Schedule usual gatherings between e-government policy makers and the concerned personnel consequently; workforces are dynamic contributors in the development.
- Build motivation by rewarding personals and agencies that play their vital role in the reforms quickly.

Cost Structures

- Government has to avoid from the services which are based on either advertising or fee. They have usually been unsustainable.
- Coherent functionalities evident and avoid to attach particulars that will drive budgets into shortfall.

- Propose and develop those projects which can be realizable with existing resources.
- Investigate previous and current available technologies then propose the projects by taking their future objectives into consideration.
- Assign an officer who will supervise the cost and expenses of projects.

Benchmarking

- While planning the stages of a project that time, clearly define the future goals and objectives.
- Assign an officer to supervise the implementation procedure.
- Ensure and recognize the funding cost, funding agencies, and departments.
- Ensure the progress of implementation; schedule audits regularly to achieve future goals timely.
- Evaluate benchmarks frequently to make sure that perfect procedures are suitable for swiftly varying technology.
- Form a data compilation system to sustain program functions to review program impact.
- Design an essential IT infrastructure and standard, which ensures current development and takes place in a consistent and incorporated manner.
- Sophisticated planning of IT infrastructure principles affect condensed development instantly and compatibility of developed systems.
- Quantitative procedures can be helpful in advancement and research.

Conclusion

Cyber democracy offers governments in either democracies or nondemocracies an ICT-based practical environment and the potential for supervising the exchange of knowledge via Internet. It is obvious that government officials have to create an interactive environment where future products means cyber democracy has to be discussed to know the latest privileges and freedom of citizens. Knowledge democracy is the basic element of cyber democracy which defends the citizen, observes the behavior of government, and depends on the principles of democracy's excellence. A question has been raised that, "will the cyber democracy be the future of Pakistan?" While assessing and evaluating democracy, its status and failure causes in Pakistan, and implications and recommendation as well as transformation practice, it is noticed that a true representation of the cyber democracy is difficult to implement. Nevertheless the revolution in Middle East and Europe will bring about a positive impact on Pakistan. The democracy in the structure of a cyber democracy is a tremendous tool for government and citizens to convey issues, solutions, and suggestions and deliver accurate information at fast speeds directly via Internet. A cyber democracy sustains and executes democratic decision and the functioning of democratic practices in a timely fashion. The major issue of concern is that the immense beneficial impact on the public's lives is at risk of being assaulted, controlled, or determinedly influenced by adversarial, cyber terrorists or concerned

parties. In this digital world, cyber threats create interference, and network defense in fragments are regular cases of cyber targets and real paradigm of surveillance attacks. From the literature, it is observed that currently cyber democracy is not capable of accomplishing democratic strategies and standards in favor of democracy. Furthermore, this type of complexity has an extreme impact on the democratic system of Pakistan, destabilizing the proper execution, positive attitude, and excellence of democracy, which depends on freedom and fairness. From the study, it is recommended that cyber democracy requires the implementation of cyberspace, and e-civilization, e-voting, virtual communities, and cyber tools perform and effectively function in cyber democracy. The cyberspace establishes the standard of increase in an advance of e-civilization. Digital information is easy to access simultaneously at various places without restrictions. Earlier information was documented either on paper or on clay tablets, which can be read and put in one place and difficult to access and manage and difficult to create duplications as well. e-voting is a primary tool to choose a democratic party and depends on three levels in the development of cyber democracy. At the lowest first level, cyber democracy undertakes no more than informative function at level one. Community discussion and meetings befits a political instrument and intensely impacts representatives and officials at level two. Residents unswervingly join in political decision-making to mark representative democracy further characteristic at level three. Virtual communities are nonplace societies which are founded on ICT tools and targets to come together about shared benefits and activities. Besides, VC interrelates ominously with fiscal and public truth. VCs along with political capabilities will develop atomic components of the cyber democracy construction. Cyber tools' reach toolbox is an application software mainly used in VCs and helpful for online democracy development. Cluster technology and Online Dispute Resolution (ODR) are supportive cyber instruments playing crucial roles in the development of cyber democracy. Cluster technology for group supports and assists group member on the web. This technology assisted for head-on conferences, which required expensive professional journeys, by web conferencing. ODR empowers resolution of argumentative problems with the usage of online approaches of intercession and negotiation. Finally, we conclude that cyber democracy can serve as a helpful building block that compliments, supports, implements, and modernizes the traditional model of democracy.

References

Abbott, J. (2012). Democracy@internet.org revisited: Analysing the socio-political impact of the internet and new social media in East Asia. *Third World Quarterly, 33*(2), 333–357. https://doi.org/10.1080/01436597.2012.666015.

Ahmed, S., & Khwaja, S. Z. (2013). Pakistan – A struggle with democracy: An analysis about the democratic quality of Pakistan. *International Journal of Social Ecology and Sustainable Development, 4*(1), 108–114. https://doi.org/10.4018/jsesd.2013010106.

Akhtar, M. (2016). *Unemployment rate in Pakistan 2015–2016*. Retrieved August 29, 2016, from http://ilm.com.pk/pakistan/pakistan-issues/unemployment-rate-in-pakistan-2012/

Awan, J., & Memon, S. (2016). Threats of Cyber Security and Challenges for Pakistan. In *11th International Conference on Cyber Warfare and Security: ICCWS - 2016*, Boston USA (p. 425).

Awan, J. H., Memon, S., Shah, M. H., & Awan, F. H. (2016). Security of e-Government services and challenges in Pakistan. In *2016 SAI computing conference* (*SAI*) (pp. 1082–1085). https://doi.org/10.1109/SAI.2016.7556112

Awan, J. H., Memon, S. A., Memon, N. A., Shah, R., Bhutto, Z., & Khan, R. A. (2017). Conceptual model for WWBAN (Wearable Wireless Body Area Network). *(IJACSA) International Journal of Advanced Computer Science and Applications, 8*(1), 377–381.

Basu, S. (2004). E-government and developing Countries : An overview. *International Review of Law Computers & Technology, 18*(1), 109–132. https://doi.org/10.1080/13600860410001674779.

Bill Phelps. (2015). *Continuous Cyber Attacks: Engaging Business Leaders for the New Normal.* Retrieved from https://www.slideshare.net/AccentureTechnology/cyber-defense-matters

Campbell, D. F. J., Carayannis, E. G., Barth, T. D., & Campbell, G. S. (2013). Measuring democracy and the quality of democracy in a world-wide approach: Models and indices of democracy and the new findings of the "Democracy ranking.". *International Journal of Social Ecology and Sustainable Development, 4*(1), 1–16. https://doi.org/10.4018/jsesd.2013010101.

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493. https://doi.org/10.1007/s13132-015-0246-7.

Carayannis, E. G., Campbell, D. F. J., & Efthymiopoulos, M. P. (Eds.). (2014). *Cyber-development, cyber-democracy and cyber-defense. Challenges, opportunities and implications for theory, policy and practice*. New York: Springer.

Directorate General. (2016). *Democracy – Homepage*. Retrieved August 7, 2016, from http://www.coe.int/t/Democracy/

Gautam. (2011). *Failure of democracy in Pakistan: Causes and solution*. Retrieved from https://defence.pk/pdf/threads/failure-of-democracy-in-pakistan-causes-and-solution.148422/

Hénard, F., & Roseveare, D. (2012). *IMHE Institutional Management in Higher Education. An IMHE guide for higher education institutions*. Retrieved from www.oecd.org/edu/imhe

Inayatullah, S. (1997). The futures of democracy in Pakistan.A liberal perspective. *Futures, 29*(10), 955–970.

Kaczmarczyk, A. (2011). Cyberdemocracy as a future product of political systems engineering. *Frontiers in Science, 1*(1), 5–15. https://doi.org/10.5923/j.fs.20110101.02.

Pak Institute of Peace Studies. (2014). *Pakistan security report*. Retrieved from http://pakpips.com/downloads/282.pdf

Palvia, S. C. J., & Sharma, S. S. (2007). E-government and E-governance: Definitions / domain framework and status around the world. In A. Agarwal & V. V. Ramana (Eds.), *Foundations of E-government* (pp. 1–12). Hyderabad: IECG.

Sekho. (2016). *Pakistan literacy rate | Current literacy rate of Pakistan*. Retrieved July 15, 2016, from http://sekho.com.pk/educational-articles/pakistan-literacy-rate/

Staff, J., & Operations, D. of. (2013). *Cyberspace Operations* (Vol. 12).

Cyber-Democracy and Cyber-Defense

34

Pavol Cabada

Contents

P. Cabada (✉)
Political science, CEIT Internship, Vienna University, CEIT Technical Innovation, Vienna, Austria
e-mail: pavol.cepino@gmail.com

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_11

Abstract

The aim of this analysis is to provide the reader with an insight into the problematic complex of 3D printed weapons and to evaluate the connected challenges for Western and Middle Eastern Cyberdemocracy in terms of security and stability. Furthermore, the analysis provides information about the rapid technical growth of the technology over the past few years and its impact on the individual empowerment, diffusion of power, and the quality of democracy. New security threats, such as assassinations, terrorism, and revolutions carried out with 3D printed weapons, will be examined along with governmental attempts to regulate their detectability. Real cases of reporter's experiments concerning the possible misuse of 3D printed weapons for assassinations and terrorism purposes will be included in the analysis. The author will take a closer look at the consequences of 3D printed weapons for the stability, security, and democratic quality in the USA and in Tunisia.

Keywords

3D printed weapons · Security disruption · Individual empowerment · Diffusion of power · Cyberdemocracy

Introduction: Research Questions and the Research Design

Societal changes have always been accompanied with technological development. Industrial revolutions have brought up significant changes to the workplace, standard of living, households, politics, and almost every aspect of life. Some, like rise of unemployment in industrial sector have been balanced by others, like persistent economic growth, creation of service sector economy, and rising life expectancy. Societies and political systems have been able to adapt differently to those changes, triggering revolutions in some political systems and shaping others into different forms. Whether the changes to the system were positive or negative, they always left a profound impact on the societies and their political systems.

Nowadays, the society is facing new opportunities and challenges with the emergence of a technology that is set to disrupt every field it touches. The progress that 3D printing has brought will have a considerable impact on our everyday lives in Cyberdemocracy. 3D printing or additive manufacturing, as the process is technically called, has evolved from being able to print simple plastic parts to advanced technology capable of producing metal parts for automatic weaponry and various components of aerial and defense industry.

The level of advancement of 3D printed weapons creates new challenges and opportunities for countries and regions alike. Files for downloading crucial parts of automatic weapons are easily accessible around Internet, with increasing number of people being able to afford their own 3D printers. Legal loopholes together with the simplicity to just download, press, and print an increasing number of items raise serious questions about the consequences for Cyberdemocracy, where Internet and

its tools have already had a huge impact as, for instance, on the Arab Spring in the past years. The mass spreading of 3D printers along with the opportunities and threats it entails creates a new security dimension in the established Western democracies and aspiring democracies alike.

The main question author wants to deal with is: *What challenges and implications will 3D printed weapons have on Cyberdemocracy in terms of stability and security?* Author assumes that 3D printed weapons will have a fundamental impact on the established as well as emerging democracies, reforming the democratic society in terms of individual empowerment, power diffusion, distributed manufacturing, governments' soft and hard power, and other areas. Author will also analyze fundamental impact on the regional and state security in terms of assassinations, terrorism, and revolutions.

First part of the analysis deals with 3D printing and its consequences on the means of production and effects on Cyberdemocracy. Technical capability of 3D technology will be analyzed and current inventions and prospects outlined. Closer analysis of 3D printed objects will provide reader with useful insight into the progress the technology is making in the world. Further, the author examines how the technology rapidly self-evolved over a period of few years.

Second part of the analysis explores the implications that 3D technology has on the Cyberdemocracy with regard to 3D printed weapons. Inventions and breakthrough events that occurred in this field will be analyzed with possible consequences for Western and Middle Eastern Cyberdemocracy alike. A closer look will be taken at the consequences on the US and Tunisian Cyberdemocracy. The USA for the reasons of becoming a primary, although not a sole, pioneer of 3D printed weapons and Tunisia as a prime example of successful Cyberdemocracy emerging from Arab Spring with 3D printed weapons becoming a possible disruption to its achievements. Regulation attempts in the USA will be outlined with consideration of their effectiveness. Author will try to point out to the connection between intended and unintended consequences of 3D printed weapons with regard to their original purpose and implications on the quality of democracy. A closer look on 3D printed weapons with regard to assassinations, terrorism, and uprisings will be analyzed.

To fulfil my goal I mainly use subjective analysis, inductive reasoning, outlining the changes that technology is bringing to the Cyberdemocracy. The main benefit of this work will be an analysis that deals with the subject of ever increasing importance of technology, mainly 3D printing, on every aspect of human life including political science. The author wants to prove that 3D printing of weapons is rapidly becoming a sophisticated technology with hardly foreseeable consequences. Since 3D printed weapons are a new emerging technology, author includes larger spectrum of areas for analysis since the topic has so far been widely neglected and insufficiently researched considering its importance for current society.

The main sources for this analysis will comprise of technology magazines and scientific articles for the description of the technological progress that 3D printing is making. For the better understanding of 3D printing's potential and technical capabilities, the author highly recommends that reader uses attached Internet links to videos. YouTube videos of 3D printing will provide the reader with profound insights

on how the technology works and what impact it will have on the Cyberdemocracy. The US report of the Department for Homeland Security about 3D printing and investigations from reporters will give the topic seriousness it deserves. The author aspires to provide his own insight into the current issue and wants to declare that he opposes spreading of weapons as he believes that their increased numbers contribute to unnecessary deaths. The same applies to the principle of 3D printed weapons.

Brief History of 3D Printing

The earliest days of 3D printing can be tracked down to Japan in the late 1980s. The technology was firstly called rapid prototyping due to the ability to create cost-effective prototypes for industrial purposes. It became more prominent when Charles Hull patented it in the USA and founded 3D Systems Corporation, one of the most significant players in the field of this technology today. First rapid prototyping system testing took place in 1987 and the technology has hit the market by 1988. In the early 1990s, the technology was evolving and thus receiving new names such as rapid manufacturing or rapid tooling. The systems availability on the market has been restrained by its technical capabilities and its high price with more time needed for the technology to mature (3D printing 2016).

The beginning of millennium was marked by the diversification of the technology. One direction led to 3D printing of products with high added value and focused on highly sophisticated technology that increasingly became visible in the aerospace and automotive sector. Second direction led to the development of 3D printers that could slowly become properties of the general public. In 2007, the price tag of a 3D printer hit 10,000 dollars, but the technology was still too expensive and too backward to make it to the households. It took few more years until the self-replicating 3D printer named *Rep-Rap* was developed. *Rep-Rap* could replicate itself by printing its own components for further replication. In 2009, the first commercially available 3D printer based on the *Rep-Rap* concept was offered for sale. By 2014, the price offered by several companies for *Rep-Rap* was starting at 500 dollars (3D printing 2016).

The last several years have been marked by substantial technical growth. The technology has been improving rapidly with the costs of the printers decreasing significantly, from 10,000 to few hundred dollars, over a short period of time. As a result, it is reasonable to believe that 3D printing will become ever more available and present in our everyday households and part of Cyberdemocracy around the world. For the better understanding of how 3D printing works, we need to take a closer look at its processes.

Additive Manufacturing and Its Processes

Additive manufacturing is often referred to as 3D printing, as it works in a similar way to a laser printer. The technology builds a solid object from a series of layers –

each one printed directly on top of the previous one (Engineer 2010). 3D printing makes three-dimensional solid objects from a digital file, by using additive processes. First step towards a printed material is via virtual design of the object that needs to be created. The virtual design is made by computer 3D modeling program or by coping of an existing object by 3D scanner (3D printing 2016).

"A file is processed by computer software and building started by laying down successive layers of material until the entire object is finished. Each of these objects can be seen as thinly sliced horizontal cross-section of the eventual object" (3D printing 2016).

The raw material for additive layer manufacturing is a powder, which can be a thermopolymer, metal, aluminum or stainless steel, and titanium 6,4. The printing chamber is generally heated to 10 °C below the melting point of the material – this ensures that the laser used to heat the powder can melt it quickly. For metals, this preheating eliminates residual stress from their processing, which can make them warp when welded. The machines' operating software cuts the computer-aided design model of the workpiece into slices, whose thickness depends on the type of material used. A blade mounted on a moving arm sweeps an even layer of the powder on top of the work surface inside the chamber and then a laser scans back and forth over the surface, melting the powder in the shape of the first layer. The work surface then drops by the thickness of the layer and another layer of powder is distributed over the surface (the Engineer 2010). This sophisticated process has enabled new means of production leading to new technical capabilities which will be looked at in the following section.

Technical Achievements in 3D Printing

3D printing has seen many incredible results in the manufacturing processes, and it has been developing rapidly in many industries. Toy industry has been using 3D printing to create odd shaped toys that children can customize and design online. Music industry has been experimenting with the possibility of printing music instruments for several years. The results were a fully functional violin, flute, and guitars, fully customized to the individual needs. A music band equipped merely with 3D printed instruments performed a first live concert in Sweden with a success (https://www.youtube.com/watch?v=U4E5SqIwa4U; EDN 2014; Lund University 2014).

In medicine, 3D printing is being used to print low-cost prosthetic parts, tissues with blood vessels, prescription medication, synthetic skin to heal injuries quicker, and many other things. Scientists are testing 3D printed heart valves in sheep, and 3D printed implants are used to replace missing skull parts. Innovative companies like CEIT Biomedical Engineering 3D printed personalized skull implants with biocompatible titanium alloy material. Customized 3D printed cranial, facial, and jaw implants were approved by the Institute for Medicinal Control (https://www.youtube.com/watch?v=hOhvHimPvcI; Just like 3D printing industry 2014).

In addition to this, 3D printing technology has moved from simple objects like toys and clothes to the production of high-value components used in automotive

industry. First 3D printed cars will be offered at the market for a price of around 50,000 dollars as early as 2016. Consisting 75% of 3D printed material, these cars are lighter, more environmentally friendly, and solid as steel despite being produced from a different material (https://www.youtube.com/watch?v=k8y4KLyLP8c; EDN 2014; Auto Channel 2015). 3D printers have been recently used in the experimental manufacture of jet engines (https://www.youtube.com/watch?v=W6A4-AKICQU) and Airbus is seeking to 3D print half of its future airplane fleet (3ders 2016; GEreports 2015). Amazingly, 3D printing has recently been used to print simple houses. Chinese private company managed to print ten simple houses within 24 h (https://www.youtube.com/watch?v=SObzNdyRTBs; New China TV 2014). China is not the only country to use 3D printing technology for construction purposes. Dutch start-up plans a first 3D printed bridge to span Amsterdam canal in 2016 (https://www.youtube.com/watch?v=pZNTzkAR1Ho). Progress in 3D printing shows how the construction works could look like in the future (Guardian 2015b).

Commercial sphere has benefited from 3D printing development in terms of decreasing costs for the manufacture, application of new processes, faster rate of production, and development of customized products in industry and medicine alike. Progress in 3D printing technology over the last 10 years has enabled people to start printing simple houses, bridges, cars, and many tools and medications in medicine. Looking at the technology few years ago, when just the simplest objects from uncomplicated materials were printed, suggests that 3D printing technology will have tremendous consequences on Cyberdemocracy. How 3D printing influences Cyberdemocracy in terms of security and societal stability will be discussed in the second chapter.

3D Printing of Weapons and Its Implications on Cyberdemocracy

Cyberdemocracy in the Context of Security and Impact on 3D Printed Weapons

Cyberdemocracy plays an important role in the context of security and societal stability, and its progress is dependent on the knowledge society and economy. "*Cyberdemocracy may be understood as a governance of democracy in the context of knowledge democracy*" (Campbell and Carayannis 2014, p. 114). The social interaction in Cyberdemocratic society sparks innovations with new forms of communication and means to share ideas. The evolution of democracy has become connected or even dependent on knowledge and heterogeneity. The boundaries of the state have become less significant and the global spreading of knowledge easier, creating new communication levels and security dimensions (Campbell and Carayannis 2014). 3D printing of weapons is emerging as a new security dimension that evolved from new levels of communication and unrestrained access to information and sharing. Whether this level becomes a contribution to the society will be a subject of this analysis.

Development of 3D Printed Weapons

3D printing has so far been mostly accompanied with its positive impact on the society. Technology has allowed to produce crucial parts for medical purposes that are difficult to produce by other means, such as skull implants. Sophisticated products for aerial industry have been produced, and 3D printing with robots has already been used to print simple houses and bridges.

Governments and public became concerned about 3D printing when it became obvious that it can be used not only for the production of commercial goods and prototypes, but guns as well. 3D printing technology is developing almost exponentially, allowing various groups of people and public to get a hold of their own 3D printer. The market grows by over 30% a year, and it is predicted that within a decade, most of the households in the USA will own a 3D printer (3D print 2014). The consequences of this development will have a significant impact on the Cyber-democracy, especially when it comes to 3D printed weapons.

3D printed weapons have initially been printed from plastic. The first weapon that received a lot of publicity was the *Liberator* from a research and development firm called Defense Distributed. The weapon was made to fire just one bullet and it usually fell apart due to the recoil forces. *Liberator* was the first step towards a 3D printed weapon that received widespread attention, mainly due to its founder Cody Wilson, who publicly declared his intention to make this weapons available to anyone with the access to Internet and 3D printer: *As long as there is a free Internet, that file is available to anyone at any time, all over the world. A gun can be anywhere. Any bullet is now a weapon* (Arktimes 2014).

In 2013, Defense Distributed posted a video showing the progress in 3D printing of lower receivers, a crucial part of automatic weaponry and the only one regulated by the US government. Version of a lower receiver firing 660 rounds without breaking has been uploaded to the Internet. In a document named *Click, Print, Gun* published by channel *Vice* shortly after Sandy Hook massacre in the USA in 2012, which claimed lives of some 20 children, Defense Distributed declared its intention to give away open source file of lower receiver for a weapon that was used in this massacre. It took just a few days and the number of downloads reached 100,000. As to the success of this open source Cody Wilson stated: *There are people all over the world downloading our files and we say good. We say, you should have access to this* (https://www.youtube.com/watch?v=DconsfGsXyA; Vice 2013).

By 2015, the lower receivers managed to fire over 1,200 bullets without breaking, and designs for rifles such as *AK 74* and *M16* were developed. Defense Distributed does not deny what the purpose of weapons manufacturing is: "*This is a battle rifle-this is to do battle*" (Medium 2015). Codie's goal envisions a working gun that could be printed in a matter of hours. In 2014, Defense Distributed released a new project called *Ghost Gunner*, a miniaturized computer controlled milling machine small enough to sit on a desktop. It is thousands of dollars cheaper compared to big computer programmable industrial tools for cutting away material. Even more importantly, it produces lower receivers from aluminum compatible with rifles. Five hundred machines were sold out in a preorder collecting 700,000 dollars for the firm (Medium 2015).

Even though the *Liberator* file was removed from the Defense Distributed website by the government, the genie was already out of the bottle and the file circles around the web. The invention of *Liberator* inspired numerous groups around the world to carry out their own research of 3D printed weapons. The first 3D printed weapons that were able to fire just one shot were printed in 2013. In 2014, young Japanese citizen Yoshitomo Imura was arrested for 3D printing his own version of a 3D printed revolver called *ZigZag* that could fire 6 bullets or 5 more than *Liberator*. Yoshitomo was inspired by the *Liberator*, so he started developing his own weapon only shortly after its introduction. It took him just a few months to develop a revolver from a gun that could fire just one shot. Few months later, another innovation in 3D printed weapons occurred when a first 3D printed rifle called *Grizzly* (https://www.youtube.com/watch?v=71mWVCrh9BM), built by a Canadian citizen, successfully fired 14 rounds (Wired 2014; Grand Power Romania 2013).

Although these weapons required removing the barrel in order to load a new round, it took just few more months until anonymous person called Franco tested a revolver with improvements enabling to fire shots without the need to remove the barrel. Shortly after this event, another organization FOSSCAD (Free Open Source Software and Computer Aided Design) printed lower receivers for a semiautomatic pistol *Skorpion* and for *AK-47*. These weapons are used by militaries around the world and are also used as assault weapons or weapons of war (Wired 2014).

Printed Metal Weapons

Although the onset of 3D printed weapons is accompanied mainly with plastic, it took just 1 year to develop a functional 3D printed weapon made of metal (https://www.youtube.com/watch?v=zJyf1IrHtcE; In the making 2014). A custom manufacturing company called Solid Concepts pioneered first 3D printed metal gun. Gun is composed of more than 30 3D printed components made with stainless steel and Inconel 625 material (Stratasysdirect 2013). With this 3D printed weapon, company aims to change the general assumption that 3D printed weapons can be made only from plastic and lack durability and accuracy. In spite of being more expensive and requiring qualified personnel, the 3D printing of metal guns is already possible: "*The whole concept of using the laser sintering process to 3D print a metal gun revolves around proving the reliability, accuracy and usability of 3D metal printing as functional prototypes and end use products*," says Solid Concepts president Kent Firestone. As to the general perceptions about whether 3D printed weapons are made solid and precise enough he adds: *It's a common misconception that laser sintering isn't accurate or strong enough and we are working to change people's perspective* (Stratasysdirect 2013).

This first 3D printed metal weapon was manufactured with striking precision producing interchangeable parts made of aluminum or steel. The advantage of such weapons is in less porosity problems and better complexities than components made by conventional methods. Solid Concepts believes that 3D printing of metal weapons is a viable solution even for the mainstream manufacturers, although it

currently requires skilled engineers for programming and maintenance of the machines. The version of a 3D printed metal gun made by Solid Concepts successfully fired over 1,000 rounds, what according to the company's president proves that 3D printed metal guns are here to stay (Stratasysdirect 2013).

The description above has focused on the sophistication and rapid advancement of 3D printing technology mainly with regard to 3D printed weapons. From the included sources, it may be concluded that 3D printed weapons have a viable future in our society more then we tend to believe. Moreover, 3D printing of weapons is advancing at a tremendous pace, developing from plastic weapons capable of firing one shot to fully functional metal weapons firing hundreds within just a few years. The next section will discuss the uniqueness of this process mainly in terms of individual empowerment, societal disruption, diffusion of power and other impacts on Cyberdemocracy, and the rights of individual.

Theoretical Consequences of 3D Printed Weapons on Cyber-Democracies

Rapid development of 3D printed weapons has been present around the world with several specific features accompanying its advancement. First of all, there is no centralized research or centralized power overseeing the development. The advancement of technology is anarchistic. It started in Austin, Texas, with 3D printed plastic weapon *Liberator*, then continued to Japan with *ZigZag*, and then started spreading to other countries around the world with the latest contributor being a 15-year-old 3D printing lethal rubber bullets. Weapons can be developed by individuals across the globe who may or may not interact with each other. The research and development of 3D printed weapons has become self-evolving and diffused, making it harder to regulate. Furthermore, it does not require a special set of skills to print out a 3D printed plastic revolver. All it takes is to have a 3D printer with a person willing to download and print files in his bedroom or small warehouse. This diffused manufacturing will enable fast spreading of 3D printed weapons in the near future with considerable implications on Cyberdemocracy in terms of individual freedom and democracy (Wired 2014).

The theoretical consequences of 3D weapons on Cyberdemocracy can be found in the origins of 3D printed weapons. 3D printed weapons originated from the anarchist groups like the Defense Distributed and other movements or individuals that detest the government's monopoly on weapons distribution. Their aim is to transfer the power to individual and transform the government's monopolistic role in power exertion.

By arming of individual, 3D printed weapons will provide society with the means of production and means of destruction, empowering individual and challenging the state. The statements from the founding fathers of 3D printed weapons such as "*Freedom of armaments to all people* or *gun makes power equal*" (Wired 2014) may be viewed as democratic and disruptive to the society at the same time. 3D printed weapons change the balance of power between individual and the state and can affect

balance subnationally, nationally, and regionally. This outlook has been described in the publication from National Intelligence Council outlining the global trends in the world as follows:

> On the other hand, in a tectonic shift, individuals and small groups will have greater access to lethal and disruptive technologies (particularly precision-strike capabilities, cyber instruments, and bioterror weaponry), enabling them to perpetrate large-scale violence – a capability formerly the monopoly of states. (Publicinteligence 2012, p. 3)

This poses a direct challenge to the state as the main power center. The defensive mechanism of the state is to restrict or "contain" the challenging power. Since the challenge does not come from other state or organization, but rather within, the governments tools to retain the power is to regulate and restrain other actors from changing balance of power. 3D printed weapons provide people with more power but new powers entail new responsibilities. From this respect, 3D printed weapons are an extension of rights but can lead to their restrictions, when masses use their new power irresponsibly. Just like Cyberdemocracy creates *New Rights and New Freedoms* in terms of control and the need for governments self-restriction (Campbell and Carayannis 2014). On the other hand, 3D printing of weapons may lead the governments to restrict individual for security purposes. Consequently, for Cyberdemocracy 3D printed weapons are a double-edged sword. They bring more freedom and power to the individuals and masses but if used irresponsibly, they will lead to restrictions from the side of government. Government's attempts to influence the 3D printing of weapons and restrict individuals from obtaining them will be discussed in the next analysis.

Political Reaction and Regulation of 3D Printed Weapons

Governments and public became concerned about 3D printed weapons when various groups and individuals started using 3D printers for other purposes than the production of harmless goods. Political reaction that was sparked after the upload of *Liberator* file on the Internet was diverse. Many progun activists claim that 3D printed weapons expand the constitutional rights of the US citizens combining the first and second amendment of the US constitution (combining the freedom of speech and the right to bear arms). Sharing of 3D printed files is freedom of speech, say the proponents of 3D printing. For this group, 3D printed weapons are a contribution to the Cyberdemocracy and the rights of individuals.

The other side of the political spectrum accuses the groups that provide open source files for 3D printed weapons of anarchism and irresponsibility. They claim that technology can be used by anybody, from children to terrorists, and become a threat to the Cyberdemocracy and the society. The US senator, a major opponent of 3D printed weapons, Chuck Schumer held a conference about the challenges that 3D printed weapons poses to the society: "*Now anyone, a terrorist, someone who is mentally ill, a spousal abuser, a felon, can essentially open a gun factory in their garage*" (Arktimes 2014). Price and availability allows various groups of people and

public to get a hold of their own 3D printer. The market grows by over 30% a year, and it is predicted that within a decade, most of the households in the USA will own a 3D printer (3D print 2014).

This development poses a serious challenge and many questions to the Cyberdemocracy:

1. Should the technology and the software for 3D printed weapons be available on the Internet as it is now or should the governments step in to prevent and regulate 3D gun production?
2. What consequences can this technology have on the societies and regions?

These questions are important not only from the technical point of view, but mainly because of their implications on the Western and Middle Eastern Cyber-democracy alike. The ability to download and print a weapon is unprecedented and moves the debate about gun control to a whole new level. Several main parts of weapons are easily accessible on the market and not prohibited from procurement, with other parts being printed from a 3D printer in order to compose a complete weapon. This created perfect preconditions for a mass spreading of weapons accessible not only to the eligible population but also to many extremists, youth, children, and other vulnerable groups. Government regulation has so far been behind the technology, although some legislation has been approved by the US Congress to counter unregulated spreading of 3D printed weapons. This legislation will be discussed in the following sections.

Regulation of 3D Printed Weapons

Several attempts have been made to regulate the 3D printed weapons in the USA. The legislative process has proven to be sluggish with many members of the US Congress unwilling to pass any regulation restricting the access to weapons. The initiative to re-enact and extend *The undetectable firearms Act* from 1988 has been successful only partially. It prohibits the manufacture or possession of firearms that are not detectable by the types of X-ray machines commonly used at airports. The new law mandates that undetectable plastic weapons have to carry a metal part in order to be detectable. However, there are loopholes that make such law ineffective. 3D printed weapons can be printed with nonfunctional metal parts that are removable, complying with the law, but enabling to pass the security checkpoints once the part is removed (Wired 2015).

The technology is progressing on a massive scale and companies are producing weapons from different components than plastic. Carbon fiber, aluminum, steel, and other components make it very difficult for legislators to keep up with technological development. When the debate about first plastic 3D printed weapons started few years ago, the technology was still backward with rapid changes coming within short period of time. One of the strongest proponents of the regulation, Congressman Steve Israel, declared his concerns about this development in the following statement:

> My legislation is about making sure that we have laws in place to ensure that criminals and terrorists can't produce guns that can be easily made undetectable. Security checkpoints will do little good if criminals can produce plastic firearms and bring those firearms through metal detectors into secure areas like airports or courthouses. When started talking about the issue of completely plastic firearms, I was told the idea of a plastic gun is science fiction. That science fiction is now a dangerous reality. (Wired 2015)

It is further important to note that the production of 3D printed weapons itself is not yet intended to be banned. What concerns the US Congress mostly is the detectability of weapons, not the manufacturing process. Even if the US Congress approved a law that would specifically prohibit the manufacturing of 3D printed weapons, there is still a way to combine the materials and parts of weapon from 3D printer with accessible components from the Internet. Any person may end up with a 3D printed lower receiver for a semi-automatic weapon with other components legally obtained from the Internet. Such combination would not be in a violation of any legislation that would seek ban on 3D printing. In other words *There are a lot of ways to make undetectable firearms and if you focus on each one you will end up with pretty ineffective legislation*, says a 3D printing-focused analyst Michael Weinberg (Wired 2015).

Department of Homeland Security in the USA is aware of the challenges 3D printing poses to national security. In its own analysis, it admits the difficulty to effectively ban the production of 3D printed weapons. A new bulletin of the Department of Homeland Security Intelligence warns it could be *impossible* to stop 3D printed guns from being made, not to mention getting past security checkpoints (Fox News 2013).

The Department of Homeland Security states that weapons can be acquired by various extremist or terrorist groups that could use them to carry out all sorts of crimes ranging from assassinations to terrorist attacks on planes. Preventing such incidences would be possible only by a thorough body search of a person suspected of carrying an undetectable firearm. Other vulnerable groups like children or people deprived of the right to bear arms could see this as an opportunity to obtain weapons without any government oversight: "*Unqualified gun seekers may be able to acquire or manufacture their own Liberators (weapons) with no background checks*" (Fox News 2013).

There are reasons to be skeptical about government's ability to successfully regulate Internet and technologies. Government's record of regulating technologies has been quite unsuccessful, naming, for instance, a case of Facebook, which reached a billion users before the governments started questioning it about serious privacy issues. In case of Internet, sharing websites can be created fast and it takes long legal action to shut them down, only to find the files uploaded on some other Internet pages. Examples of successful avoidance of government oversight and regulation can be seen everywhere. One of the most famous websites for sharing files, movies, and music Pirate Bay has been on and off the service for almost 10 years, despite website's founder's conviction and imprisonment (Vice 2013).

The regulation of 3D printing is very hard to achieve, whereas the technology has been primarily developed for other purposes. Ban or strict regulation of 3D printers

would deprive the world of its immense potential. Furthermore, 3D printing would move to the underground, where it could still pose threat to the Cyberdemocracy without the general benefit to the public. The printing of regular goods cannot be separated from printing weapons, because the procedure for the printing is same and does not require special adjustments. Downloading and even seeding of files is common across the Internet and many newspapers have contributed to this factor by reporting about it. This leads to a phenomenon where thousands of files are on the Internet, without any restriction or government oversight.

Therefore, due to the essence of 3D printing as a new tool of Cyberdemocracy, it will be hard to prevent its spreading as hard as it is to stop the flow of knowledge. It may go as far as Campbell and Carayannis describe in their paper: "*Nations don't have the power anymore of controlling and suppressing successfully the global flow of knowledge*" (2014, p. 142). This flow of knowledge empowered individuals with critical ideas and gave them the tools to spread them. In case of the Arab Spring (waves of demonstrations and revolutions that took place in the Arab world mainly in 2011 and overthrew several governmnets. Social media played an important role in this process), it undermined the government's positions and monopoly on information. 3D printed weapons, on the other hand, may empower the individual with the tools not only to undermine, but to overthrow the government as well.

From statements mentioned above and considering the governments' poor record of weapons regulation, it may be concluded that 3D printed weapons will spread rapidly to the households of Cyberdemocracy in the West or Middle East alike. Major gun rights advocates like National Rifle Association and many Congressmen oppose any restrictions on the technologies when it specifically comes to 3D printing. The sole purpose of few initiatives is to prevent the undetectability of weapons, but the loopholes and technological advancement will prevent even these regulation attempts from being effective. 3D printed weapons will be spreading and having a big impact on the security and quality of Cyberdemocracy. How 3D printed weapons open new options for foreign and domestic terrorism and how it affects Western and Middle Eastern Cyberdemocracy will be discussed in the following analysis.

3D Printed Weapons and Their Implications on the Western and Emerging Middle Eastern Cyberdemocracy

3D Printed Weapons and Their Implications on US Cyberdemocracy

3D printed weapons are going to have an impact on the Western society and the newly emerged Cyberdemocracy in the Middle East as well. The societies in the Western democracies may face several challenges arising from 3D printed weapons mainly in terms of societal stability and quality of their democracy. Year 2015 saw 1,052 mass shootings in 1,066 days in the USA (Guardian 2015a). Mass shootings that have been perpetrated by conventionally made weapons can be accompanied by increasing number of cases committed with 3D printed weapons. Current laws prevent felons, children, and other groups from obtaining weapons and the

background checks enable regulation of access to weapons. With 3D printing, weapons can be manufactured by anybody with a 3D printer and a file from the Internet. This will inevitably lead to many cases of abuse, crime, and homicides. Mass shootings in schools will become more prevalent, due to the undetectability of 3D printed weapons and the authorities may take measures such as complete body check or X-rays to guarantee public safety. Such security checks have already been a concern at the airports and they may become a normal thing in other areas of society as well (Forbes 2013).

Furthermore, protests and peaceful assemblies will become more dangerous due to individuals or groups that will try to disrupt them and instigate violence. Some revolts such as the Ferguson unrest in 2015 that saw many officers and demonstrators injured and French riots in 2005 where hundreds of police officers were injured and thousands of cars burned can become increasingly violent due to the 3D printing technology (BBC 2014). These revolts saw high injury and low death rate only due to the fact that the revolting population did not dispose with higher amount of weapons. If the 3D printed weapons had been available to the general public in these cases, then the consequences and casualty rate would be much higher. Such violent acts normally lead to harsh response from the side of the government, such as curfews, raids, and restrictions of human rights. Efforts to maintain order therefore unavoidably lead to the worsening reputation of Cyberdemocracy and their quality of democracy.

This development will only be strengthened by 3D printed weapons as there will be more threats, more reasons to restrict human rights, and more need for surveillance with government prone to regulate the population's behavior. Since September 11 the Department for Homeland Security disbursed more than 35 billion in grants to local and state police. Special Weapons Attack Team (SWAT) forces have become present in 90% of the cities with population from 25,000 to 50,000, and the number of SWAT raids has increased from 3,000 in 1980s to 50,000 by now despite the violent crime numbers going down. SWAT teams are now regularly used to raid bars suspected of serving underage drinkers, break up poker games and other small crimes. Additionally, police departments received heavy military gear and thousands of transport vehicles such as 15-ton Mine Resisted Ambush Protected (MRAP) used in Afghanistan against improvised explosive devices. The strengthening of police competences comes with police brutality and violations of human rights that leads to worsening of the quality of democracy (Economist 2015). 3D printed weapons can be therefore expected to further strengthen this process. Whether the response to the threat will be adequate is another question. The following section will consider the implications of 3D printing on Cyberdemocracy in the Middle East with closer look at Tunisia.

The Impact of 3D Printed Weapon on Tunisia and the Disruption of Government's Soft and Hard Power

Arab Spring gave rise to the phenomenon of Cyberdemocracy around the Middle East. Countries where the antigovernment demonstrations took place were

significantly impacted by social media, and communication channels like Facebook and YouTube playing a crucial, although not a sole, role in spreading of anti-government movements (Campbell and Carayannis 2014). Broad political discussions and assemblies were arranged, and pictures and videos of brutal government crackdowns became viral on the social media platform YouTube. This area, largely unregulated by government, became a space of strong antigovernment expression and undermined governments' monopoly in its main soft power, namely, the control of the media and information. With the advent of Internet and social media, peoples chance to express and organize themselves grew dramatically. People's new powers and rights have sparked a series of revolutions around the Middle East that became known as Arab Spring.

The original optimism about the democratic development after the Arab Spring has been overshadowed by mixed results. Some countries like Tunisia experience gradual transition to liberal democracy. Domestic policies of this semidemocracy have led to wider acceptance of the freedom of speech, right to assembly, and other fundamental rights. For its democratic efforts, the country has been awarded a Nobel Peace Prize. This achievement is, however, in jeopardy due to several factors. As emerging Cyberdemocracy, Tunisia faces a strong opposition from previous rulers and religious extremists alike. The development has been fragile and the government is able to maintain order only due the economic growth, rising reputation of democratic quality along with growing tourism, and political stability (Guardian 2015c).

This stability depends mainly on the economic development. Factors such as economic stagnation, rising inequality, and unemployment among youth may have a contributing impact on the spreading of 3D printed weapons. Increasing accessibility to Internet in Cyberdemocracy may lead marginalized groups to resort to violence, in order to obtain scarce economic resources and provide for their living. Worsening economic outlook combined with the frustration, particularly among the young male community, can cause social unrests and armed revolts (Guardian 2015c).

Tensions between economic classes accompanied by tensions between different ethnical groups can end up in clashes and violence, with more profound consequences for the region and higher death toll due to 3D printed weapons. There are three particular cases where 3D printed weapons pose a threat to the society and Cyberdemocracy. To this category belong assassinations, terrorism, and revolutions, all of which can be facilitated by the new technology.

Consequences of 3D Printed Weapons on Western and Middle Eastern Cyberdemocracy Alike

Assassinations, terrorism, and revolutions are the main areas where 3D printed weapons can have a disruptive impact on the Cyberdemocracy. Several cases have shown that these threats can be serious and need to be dealt with in advance. Many origins and inspirations for 3D printed guns may indicate that the direction of 3D

printed weapons is heading this way. *Repringer*, a 3D printed plastic gun made by Yoshimoto Imura, is a direct replica of *Derringer*, a gun that was used to assassinate Abraham Lincoln in 1865. *Repringer* was printed for merely 2.41 dollars, making it extraordinarily cheap and lethal enough to kill a person (Nytimes 2014). This opens new feasible options for potential assassins and terrorists. Several observers have therefore become concerned about assassinations by 3D printed weapons.

Israeli journalists decided to examine the risk of assassinations committed by 3D printed weapons. Israel had a tragic experience, when its former Prime Minister Yitzhak Rabin was gunned down at a peace rally in Tel Aviv in 1995. Reporters thus decided to put the security of the current Prime Minister Benjamin Netanyahu to the test. They downloaded 3D printed weapon *Liberator* and brought it to Israeli parliament, Knesset. The reporter passed tight security measures and went to conventional halls to assemble the weapon. Reporter later recorded on camera how he was sitting just a few feet away from Benjamin Netanyahu pulling out a plastic weapon, demonstrating how real this threat is. *Liberator* that took just 8 h to be 3D printed was not having any bullet inside for the safety concerns. According to the experts however, bullets could be easily smuggled in a sock or candy package without any detection, and furthermore, researchers have managed to 3D print lethal bullets made of plastic and rubber (Vocativ 2015).

Interestingly, Netanyahu was just giving a speech about safety and security when the experiment took place. The video surfaced on the Internet and caused scandal and questions about the security of high rank representatives. Since the gun smuggled to the Knesset was made of plastic, security dogs did not recognize it and the officials could not detect its traces of gun powder. The case of a reporter managing to smuggle 3D printed weapon through one of the tightest securities in the world urged the Israeli government to assemble a special committee that held a meeting on the threats of 3D printed weapons. The incident with *Liberator* gun was used for the presentation and examination of its capabilities. The authorities realized that 3D printed weapons are becoming a new challenge that will be hard to cope with (Vocativ 2015).

In a world full of diverse threats and challenges, a chance of a determined assassin willing to sacrifice his own life to carry out a mission with 3D printed weapons should not be neglected. The 3D printed weapons are stealthy and easy to compose and manufacture. They do not need to be smuggled through borders and their components can be manufactured on different spots without government's notice. Considering the fact that one of the best securities in the world failed to detect 3D printed weapon affirms the notion that such assassination attempts will take place in the near future.

The implications of assassinations are often difficult to predict. If assassinations on Ronald Reagan, Margaret Thatcher, and Pope John Paul 2 were successful, the strongest fighters against communism would perish before they could achieve their goals on the domestic and international stage. Ronald Reagan's assassination attempt at the beginning of his first term committed by John Hinckley would almost certainly alter the history of international relations, fall of iron curtain, and implementation of domestic economic policy known as Reaganomics. The bullet that landed in his body just inches away from his vital organs would change the course of

history. This points out to the fact that the world's development is very fragile and one successful assassination attempt can change history with a single shot (Conservativebookclub n.d.).

3D printed weapons will make the system more fragile, as some individuals will dispose with the capability to disrupt national and international order. Such disruptions like the assassination of Archduke of Austria Franz Ferdinand can lead to or become a pretext for a war. Unsuccessful assassinations, like dozens of attempts on Hitler's life, can prevent war from coming to an end. The consequences of assassinations are hard to predict, but the probability of successful attempts will grow and so will the vulnerability of international stability. Cyberdemocracy with 3D printed weapons empowers individual to be disruptive. Such actions will inevitably bring the whole region into turmoil, prompting foreign military interventions or even wars. There are, however, other areas where 3D printing can cause international tensions and escalation of violence. Some of them are hijacking and terrorism (Mirror 2016).

Hijacking and Terrorism with 3D Printed Weapons

The 9-11 terrorist attacks were perpetrated by equipment such as box cutters and small knives (Britannica 2016). Such simple and financially cheap terrorist acts have had tremendous consequences on Cyberdemocracy in terms of foreign policy, human rights, and democracy. With 3D printed weapons, terrorist acts may become more likely, whereas weapons can be assembled at spot or brought to a plane in several single pieces without being detected. As was the case of security breach in Knesset, dogs, machines, and security will not be able to counter this possibility. Coordinated group of terrorists may smuggle single shot weapons or even revolvers to the airplanes. This threat has been recognized on a legislative level as a *huge concern* by Congress representative Steve Israel who added: "*I don't want to sit back and allow terrorists to literally use 3D printers to manufacture plastic guns and plastic gun parts, put them on airplanes, bring them anywhere they want and fire them*" (Vocativ 2015). A possibility of a 3D printed weapon smuggled onto a train has been verified by reporters, who managed to bring the weapon on board of a Eurostar London to Paris train (Vocativ 2015).

Hijacking and terrorism with undetectable 3D printed weapons will have huge impact on the stability and security of Cyberdemocracy. Small plastic guns smuggled to the plane can cause tremendous damage upon economies and lead countries to intervene on the foreign soil. The 9-11 attacks, for instance, led USA to two wars in Afghanistan and Iraq that cost several trillions of dollars and were followed by rapid increases in the defense budget and violation of human rights at Guantanamo (Dailymail 2011). Massive surveillance programs under the *Patriot Act* contributed to the worsening of democratic quality in the USA. Such cases, when security takes precedence over freedoms, become easier to justify as the threat of terrorism with 3D printed weapons becomes more feasible. It is yet another example of how a technology that empowers individual and was designed to strengthen his rights may result in his restraining for security reasons.

The threat of assassination and terrorism with 3D printed weapons is serious for both Western and Middle Eastern Cyberdemocracy. There is one more area where 3D printed weapons could trigger turmoil. Uprisings and revolts like the Arab Spring may become more susceptible to violence if 3D printed weapons fall into the wrong hands. Just like *Derringer* has some interesting background story about assassinations, *Liberators* inception was inspired by similarly interesting background story important for uprisings and revolts.

Uprisings and Revolts

3D printed weapon *Liberator* received its name after a disposable single shot weapon developed by the allied forces during the Second World War. The gun was dropped over occupied territories of Europe and China in order to arm civilians, strengthen resistance, and incite revolt against occupying forces. The small single shot weapon was easy to hide and was used at close distances as a surprise attack on unsuspected smaller groups of soldiers. The goal was to "liberate" soldier's weapon after the attack and use it for further resistance against the enemy forces (Gunclubofamerica 2015).

3D printed weapons can be used in a similar way by opposition or insurgence forces in order to cause physical and psychological damage upon their adversaries. Occupation of countries would become ever more difficult as large urban and suburban areas with armed population will resist more violently against occupying forces.

Due to the technology, assemblies and protests become more dangerous to the participants and security. Peaceful protests can easily turn into bloody battles when some individuals and groups decide to use them to cause turmoil. Smaller groups of people will be capable of inflicting serious casualties over police and government forces. This in return will lead to bloody crackdowns from regime, leading to more violence and repression of democratic values.

Such security concerns have been the most problematic part of transition for emerging Cyberdemocracy such as Tunisia. Terrorist attacks in 2015 at the Sousse beach or Bardo National Museum inflicted heavy blow to democratic efforts. Although security has increased dramatically, since these attacks happened, the damage was already done. Tunisia's economy is largely dependent on the tourism with around 400,000 of ten million inhabitants directly or indirectly employed in the tourist industry. These attacks were mainly directed at the foreign tourists and caused a sharp decline of tourism in the country, bringing down one of its basic economic pillars (Guardian 2015c).

Similar disruptive acts conducted by empowered groups or individuals will be possibly carried out in the near future by 3D printed weapons. The difficulty to detect and simplicity of 3D printed weapons production can become a major problem for any Cyberdemocracy in transition. Their transition is dependent on stability, security, and economic growth, all of which 3D printed weapons can be a threat of. The growing security risks force the government to take strong security measures to prevent further attacks. Measures to insure safety lead to restriction of human rights

and downgrading of democracy status. Tensions between the government and public can escalate due to weapons made by 3D printers available to the public, which may ultimately lead to clashes, repercussions, and the spiral of violence. The fragile democratic governments may be overthrown and the Internet access that helped spark Cyberdemocracy may combined with the 3D printed weapons become a cause of their downfall.

Conclusion

The goal of this chapter was to provide the reader with an insight into a problematic of 3D printed weapons and evaluate the opportunities and challenges it poses to the Cyberdemocracy in terms of security and stability. The chapter provided information about the rapid technical growth of the technology over the past few years, concluding that the exponential growth of technologies capabilities combined with its rapidly decreasing costs will make 3D printed weapons widely available within several years. Simple plastic guns capable of firing one single shot before falling apart have evolved into lethal, customized, and difficult-to-detect weaponry firing multiple shots and capable of breaching tight security checks. Uniqueness of the technologies implications for Cyberdemocracy can be also seen in many of its attributes. As self-evolving, anarchistic phenomenon with no central power to oversee and regulate its development, 3D printed weapons are almost impossible to regulate as the US Department of Homeland Security concludes. This makes 3D printed weapons potentially disruptive to the society, mainly when it comes to the stability and security.

The three main areas mostly susceptible to the societal and security disruption as a consequence of 3D printed weapons are assassinations, terrorism, and revolutions. Assassinations that have had huge international impacts are more likely to occur due to the undetectability and affordability of 3D printed weapons. The same applies to the terrorism, both of which have proven to be problematic from the security perspective when reporters in Israel examined the possibility of assassination with 3D printed weapon, or terrorism, when a 3D printed weapon was smuggled to a train from France to England.

These modern security dimensions also impact uprisings, revolts, revolutions, and occupations with large portions of populations being able to arm and defend itself. Incidents of violence at peaceful assemblies can turn countries and regions into turmoil due to hidden 3D printed weapons and sufficient supply of armaments will likely prolong such conflicts, whereas each side of the conflict will dispose with its capabilities to manufacture weapons. As to the differentiation of the impact on the Western and Middle Eastern Cyberdemocracy, Western countries will be more impacted by possible assassinations, terrorism, and domestic revolts with Middle Eastern Cyberdemocracy becoming additionally more susceptible to the violent revolutions with the increasing chance of spiral of violence occurring as a consequence.

With regard to the government's power exertion and possible threat to the stability and security of Cyberdemocracy, 3D printed weapons may be used by

the government as a pretense for more restrictions, regulations, and surveillance, possibly undermining the original goal of 3D printed weapons to make people more independent. Consequently, 3D printed weapons are a double-edged sword for Cyberdemocracy that can be counter-productive and detrimental to its original design. Direct challenge to the states power can entail counter measures, such as militarization of police in order to meet the new security dimensions.

From the perspective of Cyberdemocracy, the development indicates that 3D printed weapons are changing the balance of power between the individual and the state, empowering individuals with unprecedented capabilities and enabling them to act disruptively upon society. Its democratization values lie within the empowerment of people, diffusion of power, and the erosion of the government's monopoly on hard power weapons distribution and control.

In this sense, Cyberdemocracy is a major contributor to the democratic quality of society. Its new communication forms create innovations and interactions that have not been possible before. It grants more power to the individual by allowing him to widely apply freedom of speech or to access knowledge and education. It gave the individual new means of socialization and representation and has arguably impacted important events such as the Arab Spring around the world. Considering that Cyberdemocracy is still at its onset, it will be necessary for political scientists to continually observe its development and impact around the world.

Altogether, it can be concluded that 3D printed weapons create new freedoms and challenges to the freedom alike. This technology makes individual stronger but at the same time more dangerous. It may contribute to the balancing of power between individual and state but also cause disruption and violence in the whole region if it falls into the wrong hands. It will be interesting to observe how the new freedoms and responsibilities will impact Cyberdemocracy from a longer perspective. If handled properly, it will become beneficial to the development of Cyberdemocracy, if not, it may lead to its downfall.

References

3D print. (2014). Over 50% of all homes to have 3D printers by 2030 – Market worth $70 billion annually. Retrieved from http://3dprint.com/915/over-50-of-all-homes-to-have-3d-printers-by-2030-market-worth-70-billion-annually/

3D printing. (2016). What is 3D printing. Retrieved from http://3dprinting.com/what-is-3d-printing/

3D printing industry. (2014). Man's livelihood restored by EU's approval of 3D printed cranial implant. Retrieved from http://3dprintingindustry.com/2014/11/12/3d-printed-cranial-implants-receives-eu-approval/

3D Systems. (2014). 3D printed "Jaw in a Day." Retrieved from https://www.youtube.com/watch?v=hOhvHimPvcI

3ders. (2016). Airbus seeks to 3D print half of its future airplane fleet. Retrieved from http://www.3ders.org/articles/20160323-airbus-seeks-to-3d-print-half-of-its-future-airplane-fleet.html

Arktimes. (2014). Cody Wilson: Troll, genius, patriot, provocateur, anarchist, attention whore, gun-nut or second amendment champion. Retrieved from http://www.arktimes.com/arkansas/cody-wilson-troll-genius-patriot-provocateur-anarchist-attention-whore-gun-nut-or-second-amendment-champion/Content?oid=3173005&storyPage=4

BBC. (2014). Ferguson riots: Ruling sparks night of violence. Retrieved from http://www.bbc.com/news/world-us-canada-30190224

Britannica. (2016). September 11 attack. Retrieved from http://www.britannica.com/event/September-11-attacks

Campbell, D. F. J., & Carayannis, E. G. (2014). Explaining and comparing quality of democracy in quadruple helix structures: The quality of democracy in the United States and in Austria, challenges and opportunities for development. In E. G. Carayannis, D. F. J. Campbell, & M. P. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense: Challenges, opportunities and implications for theory, policy and practice* (pp. 117–142). New York: Springer.

Conservativebookclub. (n.d.). The President, the Pope, and the Prime Minister. Retrieved from http://www.conservativebookclub.com/book/president-pope-prime-minister

Dailymail. (2011). The true cost of the war on terror: $3.7 trillion and counting and up to 258,000 lives. Retrived from http://www.dailymail.co.uk/news/article-2009371/Iraq-Afghanistan-Pakistan-wars-US-cost-3-7trillion-258k-lives.html

Economist. (2015). How America's police became so heavily armed. Retrieved from http://www.economist.com/blogs/economist-explains/2015/05/economist-explains-22

EDN. (2014). Wonders of 3D printing: 10 uncommon things printed in 3D. Retrieved from http://www.edn.com/design/diy/4419226/Wonders-of-3-D-printing–10-uncommon-things-printed-in-3-D

Engineer. (2010). The rise of additive manufacturing. Retrieved from http://www.theengineer.co.uk/the-rise-of-additive-manufacturing/

Forbes. (2013). This is the world's first entirely 3D-printed gun (photos). Retrieved from http://www.forbes.com/sites/andygreenberg/2013/05/03/this-is-the-worlds-first-entirely-3d-printed-gun-photos/#742497ea16c1

Foxnews. (2013). Homeland Security bulletin warns 3D-printed guns may be 'impossible' to stop. Retrieved from http://www.foxnews.com/us/2013/05/23/govt-memo-warns-3d-printed-guns-may-be-impossible-to-stop.html

GEreports. (2015). The 3D printed jet engine. Retrieved from https://www.youtube.com/watch?v=W6A4-AKICQU

Grand Power Romania. (2013). Entire 3D printed rifle the Grizzly hand firing working. Retrieved from https://www.youtube.com/watch?v=71mWVCrh9BM

Guardian. (2015a). 1,052 mass shootings in 1,066 days: This is what America's gun crisis looks like. Retrieved from http://www.theguardian.com/us-news/ng-interactive/2015/oct/02/mass-shootings-america-gun-violence

Guardian. (2015b). Dutch startup plans first 3D printed steel bridge to span Amsterdam canal. Retrieved from http://www.theguardian.com/technology/2015/jun/17/dutch-startup-plans-first-3d-printed-steel-bridge-to-span-amsterdam-canal

Guardian. (2015c). Tunisian national dialogue quartet wins 2015 Nobel Peace Prize. Retrieved from http://www.theguardian.com/world/2015/oct/09/tunisian-national-dialogue-quartet-wins-2015-nobel-peace-prize

Gunclubofamerica. (2015). The liberator pistol and the interesting history of the disposable weapon. Retrieved from http://www.gunclubofamerica.com/articles/education/pistols/liberator-pistol/

In the making. (2014). Shooting a 3D printed gun. Retrieved from https://www.youtube.com/watch?v=zJyf1IrHtcE

Lund University. (2014). World's first live concert with '3D-printed band'. Retrieved from https://www.youtube.com/watch?v=U4E5SqIwa4U

Medium. (2015). The techno-anarchist wants to make it easy for everyone to manufacture his or her own gun. But will he actually pull it off? Retrieved from https://medium.com/backchannel/cody-wilson-wants-to-destroy-your-world-ad121c8b0a6#.88mu9ayap

Mirror. (2016). Fears ISIS terrorists could soon print 3D guns for just £100 thanks to anarchist weapons fanatic. Retrieved from http://www.mirror.co.uk/news/world-news/fears-isis-terrorists-could-soon-72390

New China TV. (2014). 3D printers print ten houses in 24 hours.. [Video online] Retrieved from https://www.youtube.com/watch?v=SObzNdyRTBs

NYtimes. (2014). The rise of 3-D printed guns. Retrieved from http://www.nytimes.com/2014/08/14/fashion/the-rise-of-3-d-printed-guns.html

Publicinteligence. (2012). Global Trends 2030: Alternative Worlds. A publication of the National Intelligence Council Global Trend. Retrieved from https://info.publicintelligence.net/GlobalTrends2030.pdf

Stratasys. (2013). World's first 3D printed metal gun. [Video online] Retrieved from https://www.stratasysdirect.com/blog/worlds-first-3d-printed-metal-gun/

The Auto Channel. (2015). 2015 Geneva Motor Show – 3D printed car goes on display Retrieved from https://www.youtube.com/watch?v=k8y4KLyLP8c

Vice. (2013). 3D printed guns. [Video online] Retrieved from https://www.youtube.com/watch?v=DconsfGsXyA

Vocativ. (2015). Give me liberty or plastic death? Israeli news report sparks debate over 3-D printed weapons. [Video online] Retrieved from http://www.vocativ.com/usa/guns/liberty-or-plastic-death-israeli-news-report-sparks-debate-over-3-d-printed-weapons/

Wired. (2014). How 3-D printed guns evolved into serious weapons in just one year. Retrieved from www.wired.com/2014/05/3d-printed-guns

Wired. (2015). Bill to ban undetectable 3D printed guns is coming back. Retrieved from http://www.wired.com/2015/04/bill-ban-undetectable-3-d-printed-guns-coming-back/

Part III

Cyber-Defense

Overview of Cyber-Defense

35

Marios Panagiotis Efthymiopoulos

Cyber-defense is a most complex, yet important collective policy on security and of strategic value, that constantly develops and is implemented to secure. Currently, regional and global threats and challenges are reflective of the current situation that we live in. Variables of stability or sound change through development seem not to have become a fixed policy or understanding.

Asymmetrical threats are existential; even more so in the cyber-world. Through a new multidimensional world that has now become as complex as possible, we constantly discover asymmetries, global threats, and challenges in terms of national and international security but also strategy reflective toward the future of state of affairs in security, democracy, and development.

Within the framework of national and international security, countries, international organizations, companies and corporations, and government agencies seek to create, develop, enhance, apply, or constantly apply a cyber-defense and security mechanism, a sound and constantly adaptable protection method, from all and any kind of possible threats, whether these are infrastructural or personal.

Cyber-defense is both theoretical and tactical portions of the larger framework of national and international security. Yet, cyber-defense does not limit itself to traditional security. Rather to a cross-disciplinary approach, where, when merged with other topics such as cyber-development and cyber-democracy, the outcomes reflect the market and emerging market needs: even more so, as a multidimensional disciplinary approach of much need and use.

M. P. Efthymiopoulos (✉)
School of Law, University of Central Lancashire (UCLan Cyprus), Larnaka, Cyprus

Strategy International, Larnaka, Cyprus

Strategy International, Thessaloniki, Greece
e-mail: MEfthymiopoulos@uclan.ac.uk; marios.efthymiopoulos@strategyinternational.org

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_73

Cyber-defense emerges as a most important policy and tool. It requires a global and local regulatory and application status and framework; topics that are explored in this handbook need to be applied: further to enhance their research writing outcomes.

Writing on topics such as security or defense and even more so reflective through the cyber-world of cyber-defense or cyber-security requires sound theoretical and practical capacity knowledge of all possible security threats and the internet itself and even more so the fact that we are getting more and more interconnected day by day.

We need to be theoretically and practically aware of local, regional, and global market reflectiveness of needs. We need to be self-reliant, yet jointly interconnected and adaptable to constant technological and market changes; capacity building enablers; interoperability; network centric applicants; understanding of operations, government policies, and regulations in the world of cyber-security; private cyber-aims and objectives; and clearly the necessity to hold cyber-defense mechanisms or methods to counter any threats or attacks, digitally, conventionally, or unconventionally, at any given time and area.

Cyber-defense and cyber-security are referred to as the protection mechanisms that create infrastructure in a digital world, to protect and secure.

In our twenty-first century, and more so by the year 2018 and beyond, where the world is more e-interconnected than ever, we seek sound and robust solutions to "secure all lines of communication." There is an increasing need to adopt and adapt to new methodologies and new ideas that may as well increase the level of security as insecurity measures increase, while technology, the source of all progress, emerges to become what I call "the tool of dimensions."

New methods and actions for cyber-protection continue and will continue to emerge, to be examined, analyzed, and applied. Existing threats will continue to emerge, now and in the future.

The section of cyber-defense, analyzes, examines, and proposes specialized issues, in a cross- and multidisciplinary way; new defensive measures; strategic, political, and technical methods, policies, and operational methodologies; and how to counter current and ever-enlarging challenges and threats in a twenty-first cyber-world, while meeting global market needs and demands for a constantly cyber-resilient defense and security mechanism, nationally, regionally, and globally.

Cyber-defense interconnects itself as a discipline with the other two sections on cyber-democracy and cyber-development. It all fits in, in an era of global diversity in reasons and actions crises, from economic insecurities and instabilities to network-centric counter-operations against infrastructural threat to online democratic methods. All these publications take place at a time of constantly developing technological tools and development strategies, national and international, through visionary or strategic-led approaches.

The Section of cyber-defense is reflective to a diverse range of specializations: from human security to networked and operations interoperability and among others development of security capacity and capabilities in a e-networked world. The current section, reflects on current and future needs. It requires constant growth and knowledge of technological agility on information sharing and innovating on elements of security, strategy and safety. Cyber-defense related with cyber-security is a

specialized topic; reflecting wide-range, global by nature, strategies and tactics in and through operational preparation and implementation at all technological levels. The work produced below reflects on a wide range of interoperable new network of "interconnetiveness that is necessary to secure": The individual, our collective, our countries and our way of doing business in the 21st century (Efthymiopoulos 2016).

In war operations, therefore, "future war-like operations" and counter-measures "will be held in far more complicated than the current one, military operational environments, where battles will be dealt at multiple levels and multiple dimensions" (Efthymiopoulos 2009).

In turn "Military & Police missions, will continue to require agile and networked, well-trained and well-led forces" (Efthymiopoulos 2014).

The current section, contemplates on diverse themes of cyber-defense and security, from emerging theories and values, to legal aspects, transatlantic links, international organizations, bilateral and multilateral relations between states and global trends and attempts, and operational and tactical global challenges in a network-centric worldview context.

References

Efthymiopoulos, M. P. (2009). NATO's security operations in electronic warfare: The policy of cyber defense and the alliance's new strategic concept. Journal of Information Warfare. Published by: School of Computer and Security Science, Edith Cowan University, Western Australia. ISSN 1445–3312.

Efthymiopoulos, M. P. (2014). NATO's cyber-defence: A methodology for smart defence. In E. Carayannis, D. Campbell, & M. Efthymiopoulos (Eds.), *Cyber-development, cyber-democracy and cyber-defense*. New York: Springer.

Efthymiopoulos, M. P. (2016). NATO smart defense and cyber-resilience, working paper 1/2016. The Fletcher School of Law and Diplomacy, The Constantine G. Karamanlis Chair, in Hellenic and European Studies. http://fletcher.tufts.edu/~/media/Fletcher/Microsites/Karamanlis%20Chair/PDFs/Karamanlis_WP_May_2016.pdf.

Cyber-Security and Sustainable Development: The Case of Dubai

36

Marios Panagiotis Efthymiopoulos

Contents

Abstract

In the Security and Information Analysis community, OSINT (Open Sources of Information Knowledge) plays an essential role for national security, for its insight but also contextual process. OSINT is of low cost in acquiring information and can have its valuable use. Morally and ethically, it helps share information and knowledge, avoiding "whistleblowers." Many analysts today use among other sources open internet information sources, to draw materials that may be used for analysis or practical purposes, among them, cyber-materials, market software, conference proceedings, journals, books, profiles of people, and methodologies of advanced technical and/or technological information and open-source reports from think tanks or major institutions/organizations.

M. P. Efthymiopoulos (✉)
School of Law, University of Central Lancashire (UCLan Cyprus), Larnaka, Cyprus

Strategy International, Larnaka, Cyprus

Strategy International, Thessaloniki, Greece
e-mail: MEfthymiopoulos@uclan.ac.uk; marios.efthymiopoulos@strategyinternational.org

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_19

OSINT provides the theoretical assumption that information and flow of information do not have to be secret. Rather we argue that information needs to be practical and valuable. Open data collection is categorized in disciplines and subdisciplines. Whether we blog, browse, watch, or read specialized sources of information, we are supplied with an endless open pool of information that before we use, we need to examine, evaluate, and understand whether this is valuable and of practical use.

In an age and level of cyber-security, with which chapter will be concentrating on, is the knowledge transfer, information analysis and adoption of smart technologies, OSINT sources are deemed as important. Their validity and value of acquiring information and creating strategies and tactics based from techniques and procedures (TTPs) that can of value, an asset for enhanced safety and growth.

This chapter examines, analyzes, and elaborates the importance of cyber-security at the level of open sources, in an era of cyber-security, creativity, and sustainability, when applied in smart cities such as Dubai. The paper will process, evaluate, interpret, and analyze security, at an age of security resilience, at a time of development of mega and smart cities that need to among others be protected and thus assume future methods of decision-making importance.

Open sources are valued well, in the security and information security community. Futuristic smart cities such as the city of Dubai use extensively technology and network processes for intelligence and information structural formation. The chapter argues that a creation of big data processing center considering cyber-protection OSINT should create a new framework of security strategy and intelligence gathering information as model source for information at an age of necessary future foresight in security and intelligence affairs but also socioeconomic sustainable growth.

Questions that will be answered in the duration of this research include among others: Can modern smart city models such as the one of Dubai be used to create big data centers for open sources of collection; the aim is to enhance information gathering for safety and security purposes in policies relative to sustainable development and growth. What can the European and US sectors of security information learn through the application of this model? In and through sharing of knowledge and information on protection methods? What will the future hold once big data centers are created and applied? Will they affect positively the growth and security development of the city or cities and enhance security resilience of the state itself?

Introduction

The city of Dubai in 2018 is a smart futuristic and emerging city at the level of global smart cities (Global Smart City Leaders Praise Dubai for Setting New Standards http://www.dwtc.com/en/media-centre/Pages/2016-PR/Global-Smart-City-Leaders-Dubai [Accessed May 20th 2017]). Dubai is an innovative and phenomenal city, by definition and practice. Located in the United Arab Emirates (UAE), as the second

city to the capital Abu Dhabi, with its fine architecture, skyline, technological advances, and cultural traditions, among others, Dubai is a leading partner in physical and technological architecture, known for its capacity of knowledge transfer, management, and smart innovation. Having also established a future foresight strategic thinking in economic- and development-led methods, Dubai has in parallel developed a strong security apparatus that goes hand in hand with the Dubai Vision 2021 and the UAE Vision 2030 on safety, security, prosperity, and happiness.

Dubai's infrastructure is designed around two pillars, (1) global and local strategic growth and development through innovation and method applicability and (2) strategic security and global self-adaptability, during global and regional challenging times, while opportunity can also be considered.

The Dubai Government through its authorities and institutional agencies created a strategy of Dubai 2021 which steadily adds regional but also global recognition for the city (Dubai Plan 2021, http://www.dubaiplan2021.ae/dubai-plan-2021/ [Accessed April 30, 2017]). Under the vision and leadership of His Highness Mohammed Bin Rashid Al Maktoum, Dubai is steadily becoming a global, leading "city-state" player among global city-state players and an innovative smart city, among leading cities of the world such as Singapore and Hong Kong, to name a few.

Considering the importance of the second pillar as aforementioned above, the chapter incorporates tools and variables of and for security based on open sources of information analysis and technique methods (TTPs) used as methodological approaches toward the strategic necessity for city safety growth but also sustainability based on the government policy of sustainable growth. Open-source information collection data creation at the level of security adds operational value in security and safety and methodology approach of important data collection.

Open access information allows for government security institutions to be well aware and in the forefront of security and self-adaptability methodology, at times of great challenges but also opportunities for the future. When data collection is gathered, evaluated, and processed for the purposes of security and more so at an age of cyber-security and resilience, Dubai's future current and future challenges are envisioned, defined, and operated that render Dubai as a sustainable and growing level city providing security resilience.

Current research in 2018 reflects the significance and importance of cyber-security resilience when applied in smart cities such as Dubai. Cyber-security is an e-dimensional strategic method of protection and safety among others. Cyber-security is a tool of tactical method of technological advanced protection. Dubai is creating a cyber-resilient society and an internet security society where gathering of information data is important and where public and private infrastructure is based on security elements. Security is a target mission as Dubai is a security provider for its citizens and residents. An incorporation of data collection based on OSINT for analysis in security is achievable.

The creation of big data information can include valuable disclosed sources of information. OSINT through TTP levels of information renders information valuable. When properly analyzed, it can be of great value and information for security agencies. While security and intelligence challenges are increasing regionally and

globally, so does tactical aims and visions for discovering key methods for self-security and defense. In a city that would like to be an exemplary model of security growth, collecting and evaluating proper data for security reasons are important, while we yet "battle to establish" a "new world order" that according to Kissinger is yet to be defined (Kisssinger 2014).

Strategic aims are created with great objectives. For Dubai, the World Expo 2020 is a great opportunity and of value method, in which Dubai is to show its development identity (Dubai World Expo 2020: http://www.expo2020dubai.ae [accessed on May 20, 2017]). More so, its motto states "Connecting Minds-Creating the Future." For a period of 6 months, millions of tourists will visit the city and the country. Aiming for security and safety can be achieved through intelligence gathering-based programs, which help create a database of important and valuable sources of information (open and closed) of advanced validity through proper analysis and operational capacity to deliver a protective society.

A strategic aim is to "smart" wire the city of Dubai by 2020, to secure and cyber-secure through creation of big data source of information including closed- and open-source information with which security resilience continues to be achieved and enhanced. The setting up of the Dubai Electronic Security Authority (DESA) projects strategic and operational safeguarding methodologies applied (The Dubai Electronic Security Center http://csc.dubai.ae [accessed on May 20, 2017]).

DESA is authorized to create among others a collection of data information, open and closed sources, that will in turn be evaluated on the basis of threat and risk assessment. They should be shared next with other federal security and intelligence country agencies to secure the integrity and enhance safety of the citizens and residents. If big data collection comes along with even more information attached and e-wired, then Dubai comes in the forefront of safety, marking already the city as one of the most safest cities in the world (Dubai top lists of 'safest country in the world'. http://gulfnews.com/news/uae/tourism/uae-tops-list-of-safest-country-in-the-world-1.1910323 [accessed May 20, 2017]).

When information can be enhanced through proper TTP evaluation, then means are also provided, enhancing operational future decision-making abilities and enabling safety and security to advanced and future levels of security resilience orientation.

In this chapter, we examine, analyze, elaborate, and outline the importance of cyber-security, intelligence, and information through OSINT gathering of data for the safety and security of smart cities such as Dubai. They are new sources and methods with which we acquire analysis knowledge, for security, intelligence, and defense purposes. In the smart city of Dubai, creativity and futuristic infrastructure base requires strong levels of security providence. In turn, OSINT, as a theory and practice through TTPs, as we will explain below, is strategically located at an age of sharing of information through the web, marking intelligence in cyber-affairs as a security resilience phenomenon.

In 2018, challenges and stakes are greater and higher. "Hybrid elements" that are not yet defined as threats may be of considerable importance to intelligence minority reporting as threat assessments to come. They could be distinguished, if the market is properly evaluated through OSINT sources and TTP methods.

A comprehensive security apparatus system that meets demands on future challenges should allow big data collection based also on OSINT when evaluated for early "warning" scenarios of security threat or risk assessment as stated above. Enhanced security cooperation in the level of development and growth in smart cities such as Dubai projects not only city but also global safety measure efficacy.

Strategic Epicenter: Smart Dubai

By 2018, Dubai's modern city landscape and truly sustainable growth have become a global magnet for diverse expatriate nationalities. Dubai is a key city-source model for future city development and is an ultra-postmodern and futuristic sociopolitical and economic structural and infrastructural system that brings balance, stability, and certainly safety and security as a visionary method of success.

Dubai's technology advancement, security infrastructure, and innovative planning and action develop through a strategic development model, in which Dubai aims to lead on the global development of "emerging hubs" (Lerner 2013). Its aim is to grow more rather than become as it already is a smart city. To do so, it also needs to secure gradually to 2020 or 2021 its security resilience and posture as also a technological safety hub for all individuals, collectives, and companies and government institutions.

All successes made in the city of Dubai have a positive impact factor, for the Gulf and Arab regions. It boosts Islamic economic development and reflects the levels of success. It reflects future methodology of Middle East and North Africa (MENA) region. More so, when it is based on security, security resilience boosts effective community engagement and security cooperation with the international community and the Western world.

In Smart Dubai, necessitates a process of "e-networking or wiring" (Efthymiopoulos 2016). The strategic aim for Dubai's operational growth lays not only in the actual infrastructure but in the constant assurance of security and simultaneously growth: all services and all government institutions and authority services are e-wired to protect and serve and to support residents and help evaluate the necessity for taking part while sharing daily information. Completed with a single touch from your touch screen cell phone. At the same time, it renders the user and the resident more secure in actuality, while more data is gathered, reflecting on everyday life. Provided that Dubai does not yet hold a big data center on security, a recommendation of this research is that Dubai should create a security big data center also adding value to the OSINT shared but always evaluated by valid technique methods.

The strategic plan is to give way to true innovation and technological advancement, including safety and security. In the market epicenter of Dubai, development, stability, and security are considered as one.

Dubai is a vibrant city. It is a new smart and emerging global level and culture city, a city which competes itself in infrastructure, services, and goods and completes

with multinational and global culture environments. In many ways, Dubai is one of the new and emerging "lands of opportunities," an emerging world, and merged in a single city and completes with ideas and suggestions that are actually put to the test in a globalized and multicultural environment.

Dubai is a city of both innovation and luxury at the same time. It is a city of ultramodern architectural design in its complete infrastructure. The design of the city and its already offered services are carefully selected and constructed. It is an innovative engineered city, from its sewage system, which is applied in former desert and moving sand area in a new environment and structures that fit the needs of newly coming residents, which are ever increasing in numbers.

Dubai is a crossroad and a new world city mixing cultures and local Emirati culture and civilization that supersedes expectations on global living standards and affordable services. It offers clear lifestyle, luxury combined with architectural innovation, and high-level and high-tech services, while living expenses are skyrocketing year by year making Dubai one of the most expensive cities to live in. "Over the last decades Dubai, has applied an economic development model which is strongly pro-business, emphasizes market liberalism and economic openness, and embraces globalization..." (Hvidt 2011).

In 2018, Dubai is becoming a large and global market competitor and a hub of transport and services (Hvidt 2011). Its citizens, in its majority expatriates (expats), count of 9267 based on the UN statistics as of 2016. It is a 44 years of age country (CIA World Fact Book 9,267,000 as of mid-year 2016). Its local population, "Emirate Nationals," count according to the National Bureau of Statistics and the most recent census of 2010 as 974,997 peoples (UAE National Statistical Information on social issues and standings of living in the UAE).

The UAE's strategic vision today in its global form promotes not only UAE's heritage and culture but also a global cultural development, processes, and actions through innovation and smart thinking, planning, action, and safety and security. The United Arab Emirates comprises seven emirates, Abu Dhabi, Ajman, Dubai, Fujairah, Ras Al-Khaimah, Sharjah, and Umm Al-Quwain, located along the southeast coast of the Arabian Peninsula. The country covers an area of around 84,000 km^2 (Ibid 8, The UAE).

Dubai, which is the capital of the Emirate of Dubai, according to Hvidt, has shown through innovation, strategic investment, branding, and openness to globalization; Dubai has been able to transform a backwater, oil-based Arab city-state into a globally renowned and well-kept secret metropolis in the heart of the GCC region (Martin Hvidt, "Public-Private Ties and Their Contribution to Development," p 562, on Martin Hvidt, Economic and Institutional Reforms in the GCC by the Middle East Institute, Winter 2011, Vol 65. No 1, pp 86).

Dubai seemingly competes itself. It competes with the world in the fields of innovation and technology but also security. Dubai as New York, or Singapore or Hong Kong, among others, and visionary approaches come to being in practice, and the same thing applies at the level of expectations on security and safety.

Through architectural and engineering plans that include strategic city landscape creation, with modern social community areas and architecturally designed and business-led areas with appropriate security infrastructures, Dubai has become an example city.

In this multi-sectoral living and working environment, through diverse cultures, nationalities, and religions, in a community of local Emiratis and regional or global expats, Dubai's anthropological idiosyncrasy projects the expected growth of the city. Its future is already projected and among others safety and security assure for this future.

Safety and Security in Smart City of Dubai

Dubai is not solely an oil revenue city (Ibid 7). It is a service provider and, along the lines of it, a regional security provider. Through its executive and strategic plans of and for regional, national, and global developments, the city of Dubai in the Emirate of Dubai forecasts global innovation and technology but also safety and assures of risk assessment processes on future foresight and decision-making. It assures security, stability, and reliability analogically and now also electronically.

Dubai is a holistic model of smart cities. Concerning our research, Dubai is a model of security for the GCC and Arab regions. It is the key for security assurance success and security resilience. Its vast growth depends also on the success of security assurance. In terms of development resilience, Dubai provides the following:

- Smart technology
- Smart development and management
- Smart leadership
- Business and strategic orientation
- City and country urban planning
- Security and safety
- Global competitiveness
- Accelerates the future of things

Key performance indicators for Dubai include the following elements: diverse sectors of innovation collaboration and strategic management. In turn, its strategic visionary capacity to create and operational ability to deliver allows for Dubai to craft and or predict the future. That includes all elements and variables for growth and safety for the Emirate and the UAE.

Dubai positions itself globally, as a global epicenter. As already stated, this includes technological and socioeconomic growth, agility in security, resilience, and business security continuity. According to the Ruler of Dubai, His Highness Mohammed Bin Rashid Al Maktoum, all residing in Dubai and sharing the vision of the city and the UAE, should "Utilize & Not Miss Opportunities."

Security for Dubai reflects both regional and global interconnectedness, through its federal government based on Abu Dhabi, the capital of the UAE, as earlier stated. Security is applied, and eligibility criteria for those to reside in the UAE and in specific in Dubai apply to all those visiting and/or residing. Per the residents or citizens, security is necessary. Security methods are coordinated efforts, using all

technological agility tools that just make sense, and provide accuracy of knowledge and information per resident and citizen, profiling the importance and the necessity of this person to reside and the support that they will provide toward the development and growth of the city and the Emirate.

Dubai offers actual and applied safety and security at third- and fourth-dimensional levels. It allows for strong security resilience, in both personal and collective investment methods affordability. Security applies to the individual, the family, and all other collectives. When security is assured, but also constantly enhanced, the resident, the citizen, the visitor, and the investor feel also assured.

Elements and tools of security are constantly updated. Security is constantly enhanced. It needs to be evaluated at periods of time, examined, and analyzed, and new security measures and tactics need to be acquired and taught, more so, when security reflects intelligence or otherwise is stated as methods of gathering of information for analysis on security and today also applied in multidimensional ways.

Dubai constantly invests and injects new ideas and issues for security capacity building methods and techniques. More so it invests academic-led programs created and/or tailored in the UAE and through them invests in human capacity training that provides affordable security resilience. In turn, all programs and methodologies should be revenue based for the growth in safety in among others the city of Dubai.

Elements used to analyze security resilience for the Emirate of Dubai should be based on sources of information that are also open for intelligence analysis. All programs related with security, education, resilience, awareness, and development should become a reflection of all OSINT community-based information gathering of data. In a smart city led by a strategy of cyber-security protection, gathering of open-source information is important. TTPs will evaluate its value and commitment to security, affordability, and risk assessment through proposed measures, thus complementing current strategic development on future security foresight for the city of Dubai.

A Note on the Cyber-Security Landscape of Dubai

It 2014, the Vice President and Prime Minister of the UAE and Ruler of Dubai, His Highness Sheikh Mohammed bin Rashid Al Maktoum issued law no 11/2014, establishing the "Dubai Centre for E-Security" (Ibid 5).

The center is a corporate body and enjoys a legal status and financial and administrative autonomy. It aims to protect information, communication networks, and government information system in Dubai.

The Electronic Security Cyber Center (Ibid 5) operates on the basis of providing the technical tools and efficiency and logistical support for all government entities in Dubai while at the same time protecting the citizens, residents, and tourists arriving and/or residing in Dubai. It is tasked to go in parallel with the strategic goals of Dubai to continue being a safe and developed city, a strong hub, and a center for trade, culture, and high standard of living.

The capability framework includes coordination with all government entities, cyber-crime protection mechanism, and a proposed center for e-regulations on e-security and

safety. Knowledge and awareness are complementary efforts, which will allow the center to take part and jointly cooperate in multi-educational levels of cooperation.

The center operates as a coordinating and regulatory evaluation authority, which upholds the national and city laws, in order to follow the rules and regulations, to complete tasked cooperation with each authority, and to reach a security-level approach toward e-security and e-governance protection methodology.

The center will be operating based on a strategic plan as of 2017, to counter possible current or emerging threats. Considering the framework policy of "Dubai Future Accelerators", its mission will be to aim to foresight the future in security and among them cyber-resilience in security-led affairs and to secure and implement methodology for all government agencies as well as business organizations and institutions to protect, to interrupt, and to secure the grid networks, whether these reflect the communication networks or the information networks coming in from each system (Dubai Future Accelerators, https://dubaifutureaccelerators.com/en [accessed on May 20th 2017]).

The center complements efforts of the Emirate National Electronic Security Authority (NESA) to which it "liaises" and collaborates with. NESA is the protective authority for all national security authorities in the United Arab Emirates (National Electronic Security Authority, http://ebdaa.ae/our-services/national-elec- tronic-secu rity-authority-nesa.php [seen on May 20 2017]).

All of the above concentrated have already allowed for the center to become among others a regulatory body accreditation, which is obtained by decree by the ruler of Dubai and tasked to both implement protection practices such as to collect and evaluate data, and more so now it will need to develop bid data collection also based on OSINT. Such achievements will in turn allow for the city's e-security plan of development, considering the needs for continued enhancement of security, equally leading to economic prosperity and sustainable growth.

State of Innovation: OSINT and TTPs for Dubai's Security Resilience

Dubai moves ahead in becoming a "city of innovation" (Ibid 8), applying what is called as "accelerator methodology" (Ibid 16) in both technology and infrastructure but also human capacity building. Dubai acquires knowledge transfer on a diversity of disciplines and specializations. It innovates and acquires innovation in the fields of logistics, procurement, banking, transport, and trade, among others in disciplines of security and other interrelated disciplines that we are concerned with in this paper such as intelligence, cyber-security, and operational capacity building. These are some of the success factor stories of the smart and global city of Dubai.

Concerning creativity in security affairs for Dubai, limitless opportunities are singled out. In 2017, key characteristics for Dubai's security growth concentrate around a smart cyber-resilience security and future foresight on possible security challenges. It reaches out on and about policies of practical importance. The creation and

implementation of a cyber-security strategy that projects interoperability and interconnectedness, with current security affairs, will allow for new protection methods committed to smart technologies and smart city as Dubai. The Dubai Electronic Security Authority holds a specialized policy process, procedure, and applicability. Its strategy application will be presented within 2017. The strategic objective is to find methods to enhance e-security apparatus, to create a role of supervision and operational contribution to the law enforcement and protection methodologies and agencies, and more so to establish a leading role of data-based collection on both closed and open sources.

Concentrating on the element of OSINT for security resilience in Dubai, we should stress that the "state of innovation" of Dubai necessitates OSINT to be proportionally applied on assessing and managing current and future risks or threats, while the city develops. The city is a smart hub of development based extensively on technology. Technological advancements necessitate more close attentiveness but also preparedness and awareness. Protection safety methods, do require preparation; they do require "big data" archival database creation, with which we can achieve information knowledge and resilience, so as to achieve data, information and tactical security.

OSINT is already applied in many organizational levels of the private market industry, "due the relevancy of building an internal, specific know-how in this area" (http://www.expertsystem.com/what-is-osint/ [Accessed on May 20th 2017]). The right tools for OSINT, combined with the right skills of teams, are "increasingly OSINT-oriented can help organizations become more and more effective" (Ibid).

From Open-Source Intelligence to Open-Source "Semantic" Intelligence

Organizations are increasingly turning to what is called "semantic technology" (Ibid 20). It helps gain intelligence from multi-streams of unstructured data and information they manage daily. That is why big data collection is so important at this stage for Dubai. Security resilience for the city requires constant stream data on profiles, operations, and activities among others that may be used for analysis purposes considering the strategic need to foresight future challenges and threats. "Unlike keyword technologies or cognitive computing systems based on statistics, semantic technology is unique in its ability to approach the automatic understanding of a text" (Ibid 20).

Creating a big data center for OSINT information on security, cyber-resilience, and protection strategies in Dubai equally means applying semantic understanding to OSINT. It will allow for an increase in intelligence operational risk and compliance analysis. It will also provide the opportunity to security analysts to govern over all dataflow and information**,** identify possible current threats, create a probability factor through a minority report, and develop a clear threat assumption future planning based on intelligence and OSINT info "picture."

Tactics, Techniques, and Procedures (TTPs)

TTP is a compliance method against current cyber-threat, more so, a tactic and technique of evaluation of the current OSINT information that flows. TTP can be used as a tool for what is called penetration testing. It is an effective measure for security information and intelligence analysis. TTP is important as it reflects non-traditional elements or symmetries on war and peace, intelligence gathering, and operations. TTP supports analysts for OSINT information relatively when reflecting or referring to cyber-security elements. Cyber-security measures reflect methods against threat actors. They protect the network whether private or public.

In OSINT sources, there is a threat actor. Between the open, deep, and dark areas of the web, a massive quantity of relevant data is available to anybody who knows how to find it. TTP in this level works as a defense zone that collects and stores threat data automatically, even more so, when OSINT sources provide information that may flood data without much importance or use.

Lessons Learned

Dubai's smart city policy on security and strategy, intelligence, and information data collection is counting on the center on cyber-resilience that will operate in facing current but also establishing threat assessment on future e-challenges. As Dubai's security status and apparatus needs to continue to provide assurance and agility, there is a great opportunity for Dubai to lead the e-world of smart cities among others in cyber-security-led affairs.

- Dubai should create a center for big data collection that will be based on OSINT and TTP evaluation and self-defense methods.
- Analysis center of OSINT information that will be constantly evaluated to support intelligence analysis and flow of information for future risk and threat assessment foresight.
- Sharing of valuable information through flow of minority reporting based on both closed and open-source data.
- Awareness on security- and education-led programs on security and intelligence for the benefit of the United Arab Emirates.
- Resilience and interoperability processes to be applied for international standardization activities, so the flow of information can expand and be shared with international agencies.

"According to Frost and Sullivan, cities which become smart, will become shareholders of a market of potential global revenue to be shared, which counts according to the report $3.3 trillion by the year 2025" (Ibid 8). Making knowledge, innovation, and security application a must, Dubai should be expected to become a complete self-secured but also big data protected e-city by 2020. It should coincide with the primary goal of the city's success toward the upcoming World Expo.

Recommendations

Dubai needs to meet the trajectory requirements of an e-safe environment by 2021, which will mark also the completion of the currently ongoing strategic development plan of the city. It will give way to an upcoming strategic agenda of 2021–2028, on concentration also on security-led issues. Specific challenges will be raised that will be of electronic and technical necessity and importance. Thus a big data collection and a center for analysis performance are of importance.

Acknowledging current and emerging international and geopolitical challenges, Dubai as stated already stands out as a magnet and a hub of innovation but also opportunity. Through valuable establishment of research methodologies, a "token" for an e-secure framework is already in place and being built. Through OSINT information, security-led protectionism will expand adding value to current efforts to protect valuable information and infrastructure. It will also help create a sustainable future technology for institutions and organizations operating in the city of Dubai, making and marking the city as an innovator on security production but also appropriate risk assessment analysis and formation.

The center should concentrate on an actual agenda of security threats and vulnerabilities as they exist today but also will possibly exist in the future; and OSINT can help form and shape the final security report. More so, through the TTP, we may protect the flow of OSINT information while enhancing protection methodology against (a) application vulnerabilities, (b) malware, (c) hacking, (d) third parties/mirroring, (e) organized crime, (f) cyber-terrorism, (g) cloud-based services, (h) against state-sponsored acts, or (i) e-ransoming (In 2013, (ISC) 2 Global Information Security Work force study by Frost and Sulli- van consulting in Partnership with Booz Allen Hamilton and (ISC)2, by Michael Suby Global Program Director on Information Security, file:///C:/Users/Marios/Downloads/2013-ISC2-Global-Information-Security-Workforce-Study%20(3).pdf [seen on 20 May 2017]).

Cyber-attacks when assessed and evaluated through OSINT, in multilevels through multi-scenarios, can afford possible assessment of the future in smart city such as Dubai. Awareness through educational programs on intelligence, sharing and gathering of information, projection planning, game theories, and future challenges will enhance learning and operating efficiency.

Conclusion

In a period of export-developing models and sustainability, according to the rulings and the wishes of the leadership of the United Arab Emirates, the Emirate and city of Dubai are role models to the MENA region to start with, practically more can be done to assure smart city, security, and defense for Dubai, leading to the World Expo 2020 and beyond.

A smart city and therefore smart securitization of all e-networks and infrastructures will lower possible current costs in daily operations and human capital. Any

possible cost will be associated with the value of services provided. e-security and e-defense will become part of the smart city allocation of revenue, rendering more assets to the city of Dubai, while it will allow for global cooperation and sharing of information and from a point on expertise work.

This research chapter focused on multidisciplinary elements reflecting sustainable growth, security economic prosperity, and electronic development methods. It examined, analyzed, and elaborated on the importance and necessity of OSINT in an era of cyber-security and cyber-intelligence, when applied in smart cities such as Dubai. The research evaluated, interpreted, and analyzed OSINT strategically, at an age of cyber-intelligence and security resilience.

References

Acuto, M. (2010). Global cities: Gorillas in our midst. *Alternatives: Global, Local, Political, 35*(4), 425–448. https://doi.org/10.1177/030437541003500405.

Acuto, M. (2010b). Alternatives. *Alternatives: Global, Local, Political, 35*(4), 425–448.

Ben Brik, A., Rettab, B., & Mellahi, K. (2011). Market orientation, corporate responsibility and business performance. *Journal of Business Ethics, 99*(3), 307–324.

Efthymiopoulos, M. (2016). Cyber-security in smart cities: The case of Dubai, Springer. *Journal of Innovation and Entrepreneurship, 5*, 11. https://doi.org/10.1186/s13731-016-0036-x.

Kisssinger, H. (2014). *World order*. New York: Penguin Books.

Hvidt, M. (2011). Economic and institutional reforms in the Arab Gulf countries. *Middle East Journal, 65*(1), 85–112. Middle East Institute.

Lerner, J. (2013). The boulevard of broken dreams: Innovation policy and entrepreneurship. *Innovation Policy and the Economy, 13*(1), 61–82. The University of Chicago Press.

Meyer, K. E., & Brysac, S. B. (2011/2012). Kerala: Multiple improbabilities. *World Policy Journal*, *28*(4), 60–69.

Protective Function of Digital Forensics

37

Dusko Tomic, Eldar Saljic, and Hana Korac

Contents

Abstract

We live in a time of rapid and intensive changes, where information is seen as both the main resource and a critical infrastructure of a state. Necessarily, these changes also carry around retrograde processes, which manifest themselves as misuse of not just communications but of everything inside a communicational maneuver. In such cases, the protective role of digital forensics is both inevitable and highly necessary. In this paper, we elaborated the function of mobile telephony and its digital forensics, because right now, there are more than seven billion devices being used globally, more than there are people on earth.

Keywords

Mobile telephony · Digital forensics · Security · Protection

D. Tomic (✉) · E. Saljic
American University in the Emirates, Dubai, UAE
e-mail: dusko.tomic@aue.ae; eldar.saljic@aue.ae

H. Korac
Ministry of Internal Affairs, Sarajevo, Bosnia and Herzegovina

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_21

Mobile Device Forensics

The goal of mobile device forensics is to recover data (evidence) from mobile devices by using different methods, where each method has its own conditions. When these conditions are met, the problem of having collected invalid data is solved, and data that has been collected this way can be used as evidence in judicial proceedings and other processes. The practice has statistically shown that there are many cases where such data was the key evidence.

Mobile device forensics differ from desktop computer forensics, because mobile devices are working in different networks, which further impacts the process of delivery and keeping and processing the data. Apart from collecting data, mobile device forensics also values the connection between the process of collection and device hardware. This way, the user gets a feedback which gives him complete insight in the organization of the mobile device and the spectrum of his capabilities. All processes are being conducted step by step, which ensures more security and validity of the output results.

Data Collection from Mobile Devices

The way in which data is being collected from mobile devices can be different, depending on the type and condition of the device, and can even be different if we take into account the condition of the data we're trying to recover.

Mobile device forensics, a type of forensics which falls under computer forensics covers cell phones, smartphones, tablets, personal digital assistants (PDA), and GPS receivers. All of these fall under computer forensics. Because mobile devices are becoming more and more of an instrument, meta, or a recording tool for a crime, they have become an item of special interest in a criminal investigation, a civil lawsuit or in the collection of information data. Some even go so far as to claim that mobile devices contain more evidence per byte than traditional computers. Most smartphones now come with sophisticated apps and built in cameras, lots of storage capacity, and fast network connection, which leads to a great computing power being easily available for users. Despite mobile device forensics also taking into account eventual deleted data, in criminal or civil lawsuits, these processes are also used in applications outside the court. Data that can be extracted from these devices includes call history, sent and received messages (SMS) and multimedia messages (MMS), contacts and phone numbers, emails, photos, video recordings, geographic and GPS information, network settings, web history, voice messages, social network information, application history, log files, and other data that can be found with smart applications.

There are many commercial and open-source products for the collection and analysis of data from mobile devices, from program packages for the camera that takes a screenshot to products that analyze the database and the hardware to physically examine chip types (Fig. 1).

Fig. 1 Products used – (*1*) Cellebrite UFED, (*2*) Micro Systemation XRY (Yong et al. 2012)

Mobile device forensics requires processes and tools that can extract information from at least six different mobile operative systems, including iOS, Android, Windows mobile and thousands of other mobile phones, tablets, and GPS devices.

Even if the forensic can access the physical memory, the analysis of the binary storage may require old-fashioned analysis with hex editors (e.g., HXD Hex Editor), standard tools of computer forensics, and a regular term analysis. For example, Android phones have important fragmentations and variations of their operative system, which makes the location of common data within the operating system pretty difficult. Even Apple iPhone devices have different data depending on the version of their operative system and if the phone is jailbroken (freed from the software limitation of the manufacturer – Apple).

Many "dumb" phones on the market store contacts and SMS messages on the SIM card, while pictures or video recordings are being stored locally on the device. Tablets behave the same like phones in terms of collecting forensic data. Because of the large amount of personal and work related data on mobile devices or that can be extracted from device information, security and privacy of these devices seem to be a big challenge.

Apart from putting information about a user on a phone, operating systems also store information without the knowledge of the user. In April 2011, for example, Apple gained large media attraction after it has been shown that iPhones have been collecting detailed histories about geographic location from users in an unprotected database. With a simple extraction, the forensic can create a geographic map of all the places the iPhone and its user have visited, the key lesson being that sensitive data in smartphones should be coded.

USB and memory cards have some characteristics that differentiate them from standard storage units, like physical size, work type, etc.

Unlike hard disk drives, which are most often inside a computer and in most cases contain only digital evidence, portable drives have several types of fingerprints, just because they are handed over several times. But, it's also very easy to determine who has held the storage unit last. Handling these devices and extraction of all types of physical evidence from it is very important before the digital forensic process itself. Even the smallest physical damage to the connectors can be a proof that will either free or convict a suspect.

There have been many global cases involving child pornography, where the forensic findings, which, based on microscopic signs of wear could lead to the conclusion that specific memory cards have been used in a specific camera have been accepted as evidence. The position of connectors, the way the storage drive has been plugged into a device, and even the space where the memory card, for example, was kept mark it with different signs of wear. Even two photo cameras from the same series will leave different markers on a storage unit.

The following procedures are needed in cases where data collection from damaged flash memory units needs to be collected or deleted data needs to be recovered:

- Separating the memory chip from the damaged device
- Reading of the memory sectors and the creation of an identical memory "image"
- Detection of the specific mix from different memory sides
- Deleting the mix
- Applying adequate algorithms in order to connect all sides into one single content.

After this process it's possible to logically access the data. However, it's necessary to configure parameters for the applied file system (in 90% of the cases, it's FAT12) and restore the logical structure and copy files afterwards. There are exceptions of the described procedure. Mini and micro SD cards do not have a controller; some devices even have encrypted pages in the memory which are impossible to decrypt if the controller fails. The data is stored to the memory completely different from the data on hard disk drives. The whole memory is partitioned to several "pages," where the size of the page and the storage process depends on the type of the algorithm applied. Also, the layout of the pages within the memory is not linear, depending on the type of applied algorithm, where there can be many variant mixes of the same page (Datasolutions 2013).

Regarding the forensics of personal digital assistants (PDAs), the process of forensic information gathering is very similar to the data collection from other similar variants. Basically, the process consists of four fundamental steps:

- Examination
- Identification
- Collection
- Documentation

These are the steps on which any forensic investigation of different devices is built upon.

At first, it's necessary to identify the evidence sources. In this case, it can be the device itself, the device body, the energy source, or any other peripheral device that was interacting with the PDA or that the PDA was synced with. After the collection of evidence from the exterior body of the device, it's necessary to investigate the device from the "inside" (process the memory locations and the operating system, like it's described in the smartphone section).

Portable music devices are treated similarly to simple "hard disk drives" from a computer because of the nature of their system. Like the practice with personal computers and their forensics has shown, it's necessary to create a system image, because it's not recommended to work with original files. In order to maintain the integrity of the files, forensics use "hash" as a fingerprint, which would guarantee that the files haven't been changed in any stage of image creation (Reyes and Wiles 2007).

Tools for Collecting Evidence

The tools being used to collect forensic data from mobile devices differ according to the device type. Thus, the same tools are used for similar devices.

Some of the most popular tools for collecting data from mobile phones, GPS devices, and tablet computers are as follows (Franc 2013):

- Cellebrite Universal Forensics Extraction Device (UFED)
- Oxygen Forensic Suite 2012
- Paraben Device Seizure
- Micro Systemation XRY
- Logicube CellDEK

These tools use the same protocols like the non-forensic tools of the manufacturer, but they don't implement the commands that explicitly modify the content of memory on a mobile phone. The common thing unifying mobile phones, GPS devices, and tabled computers is that they are all based on the same operating system, which means that collecting data is conducted in a similar way. Manufacturers follow the development of their models constantly and fill their basis constantly with new models that appear on the market.

Regarding PDA devices, it can be said that there aren't that many tools that can be used for forensic investigations. The most common tools are PDA Secure, PDA Seizure, and EnCase.

PDA Secure offers better protection through a password, together with an encryption, an unlocking device, and the possibility of deleting data. It allows the administrator to have more control over how the devices are used within networks. Other than that it allows for the setting of time and the tracking of time for information such as logs onto a network, infrared transfer, and all the apps used during a specific time period.

PDA Seizure is a complete tool that helps with "seizing" the device. It operates within the Windows ecosystem and can separate the working memory (RAM) and the permanent memory (ROM). It has a graphic user interface (GUI) that is easy to use and uses tools that are necessary for exploring databases within the device. It supports different platforms on which the forensic can gather and investigate information on devices for both Pocket PC and Palm operating systems.

For the analysis of music devices, any tool that works with FAT32 systems can be used. In other words, you can use any tool for forensic collection of data from personal computers: Guidance Software's EnCase, AccessData's FTK, Brian Carrier's Sleuth Kit, Paraben's P2, etc. (Reyes and Wiles 2007).

Examples of Collecting Data from Mobile Phones

Mobile phone forensics can be separated into memory location forensics and SIM card forensics. During the process of data collection from a SIM card, it can happen that a PIN (personal identification number) code is required.

We differentiate two types of access to the acquisition of data from mobile phones (Telekomunikacije 2013):

1. Acquisition on a logical level is the collection of data from the mobile phone's memory. In order to collect data in this way, it's necessary to have knowledge about any phone being processed in order to minimize the number of false steps (specifically the steps needed to conduct changes on the phone itself). Because of this, SMS messages, which for a forensic analysis are very interesting, represent a very demanding segment of manual acquisition, just because it's necessary to enter the entire unchanged content of each message into the report. Going further, the same nature of modern organized crime shows us that very often phones are seized from foreign citizens, which contain a large number of messages in the native language of the owner, and this fact further prolongs the acquisition. It's also to note that, when you look at organized crime, the definitions of organized crime and terrorism overlap. As Saljic and Djordjevic stated: "Both groups frequently operate in decentralized cell structures, tend to target civilians and use similar tactics such as kidnapping and drug dealing." (Saljic and Djordjevic 2011: 285)

Applications on phones do not focus on systematically showing all data that forensics can use, so usually the most time is spent on going through different menus and submenus. One example, again, could be SMS messages: to the details of those messages, like date, time, and the prepaid number of the sender, you can get through submenus, because it's only the details of the message that are being displayed (most often only the name from the phonebook).

Manual access is used only in cases of searching for specific digital evidence on a device or if there is no other way of access the mobile phone and collect evidence (Casey 2004). Cheaper and newer models of mobile phones, which are not sold by

carriers and often do not even have an interface for interactions with the device but possess large capacities for storing SMS messages, are a special challenge. Eventual changes that can occur (e.g., receiving calls or SMS messages) during the manual acquisition, while the phone is on, are being interrupted with a Faraday cage (most often in the form of special bags which block the electric field) or with the cloning of a SIM card.

2. Physical acquisition is the copying of the entire memory, bit by bit. This allows for the collection of data from areas which the operating system does not locate or otherwise known as the recovery of deleted files. Connection service acquisition is currently the most widespread method now. This is the basis for forensic tools which use protocols to send commands and receive data for communications with services, such as open protocols like AT Command Set, SyncML, or OBEX, all of which are already outdated, or vendor protocols like Nokia FBUS. There are also developed tools that allow programmers to create application which use the mobile phone service without implementing basic protocols. The connection service acquisition is conducted by using two sets of tools.

The most common tools used are tools for mobile phone manufacturers or independent programmers, which allow for collection of specific sets of data and are designed for synchronization with the computer or other mobile phones or the creation of reserve copies and not forensic tools. A common consequence of inadvertency while using these tools is the serious destruction of the consistency of digital evidence, and the collected data is most often in such a form that it can't be used for creating reports (there have been many problems with the Nokia PC Suite (for different vendor models), which show SMS messages in a table, but does not allow for them to be copied nor does it permit the exporting of any data). Other forensic tools are the already mentioned tools for information collection.

The mentioned access types are applied in different methods for the acquisition of data from a mobile phone:

– Connection agents are small programs (e.g., the connection agent forensic tool XPY installed on a Nokia N95 phone is 34 kb big) that are placed on target phones in order to establish a connection and the exchange of data between the phone and the forensic tools. Such access uses the client-server architecture with the agent acting as a server. Without that, the tool couldn't get to the data from the memory of a mobile phone. Because the agent plays the role of a connection service, the acquisition of data is similar to the before mentioned one. This method is largely used on smartphones. The main problem is that, no matter how small the software can be, the program must be placed onto the memory and therefore alters it.
– Direct access to a mobile phone memory is most often adapted to the forensic principals but is also the most demanding method of acquisition (Willassen 2005). This method gathers data on the physical level and makes forensic copies of the entire memory of a mobile phone possible, regardless of the size of the

occupied memory space. The direct access also ensures the recovery of deleted or partially expelled entries, as well as the circumvention of security measures which would make the access to the data on a logical level and the other methods of acquisition impossible without interventions, while the impact of the security breach to the digital integrity of evidence would be unknown. Another advantage of direct access is its independence from the question if the mobile operating system would ensure valid results of the acquisition, something that is not the case with other methods. There are three different types of direct access (Keonwoo et al. 2013):

- Removing the memory chip from the printed motherboard of a mobile phone and reading its content (for a criminal investigation, this might sound like a risky procedure, because the chip can be damaged by the temperature used to separate it from the board and with it the digital data).
- The use of ports for a JTAG (Joint Test Action Group) test , standardized procedure for the testing of internal connections on a motherboard and the sub-blocks inside an integrated circle for the creation of a complete forensic copy of the content from the replaceable and non-replaceable memory of the phone. The problem with this is that on newer models, the ports are harder to find and to access, because it's often hidden by manufacturers.
- The use of flasher tools for programming the device memory (EEPROM or flash drives) or for diagnostics or failure detections (something very frequently used by manufacturers). The problem with this tool is that in specific cases, it can only read a portion of the memory, and every manufacturer has its own, different access interface, which makes it impossible to achieve widespread appliance.

Applying any of the three abovementioned methods of direct access requires a high level of technical education and knowledge, as well as laboratory working conditions. The biggest flaw regarding the other methods is that the job is not completed with the acquisition – it's still needed to analyze raw data and extract complex and useful information from it, also known as evidence, which then could be presented in a reasonable form (Telekomunikacije 2013).

- Collecting data from a GSM network. First, with this method, you could gain detailed information about the achieved communications between devices over a long period of time. These are much more reliant than those found on the phone, and often this method of acquisition is used for validation of data collected with another method. We can conclude that there is no ideal method for acquiring data – instead, compromises between effectiveness and efficiency have to be made, or, in other words, the priority needs to be determined in regard to the operational information, and for each case, a different method needs to be chosen. Modern forensic tools combine several methods and approaches, with the intent to change as little as possible inside the phone but to, nevertheless, obtain as much digital evidence as possible. With the goal of providing proof that the digital perseverance of the evidence has not been damaged, the person that conducts the acquisition must document all activities in the work with a mobile phone and

minimize the interaction with the device. The more interactions are being conducted, the more complicated it is to proof that the actions did not compromise the digital evidence (Mokhonoana and Oliver 2007). If the mobile phone has been put in a sealed envelope during the seizure, and the defending attorney or the suspect is present during the opening and the acquisition, then the conditions have been met to use this digital data as evidence, because the doubt in eventual damages done to the evidence material has been lifted.

Micro Systemation XRY 5.1 (Viaforensics.com 2013)

This tool for acquiring data from mobile phones, GPS devices, and tablet computers can be used for both types of acquisition (physical and logical). It's based on a Wizard that leads the user through the process of data collection. All extractions (physical and logical) are stored in a XRY file that stays in that format for security reasons. It is then possible to extract reports from this file, which can be shown in Word (.doc), Excel (.xsl), Open Office (.odt), or PDF formats. It is also possible to choose which evidence will and will not be included in the report, and there is a reader that allows a third party to actually get involved into commenting on the report while keeping the integrity of the data. The latest version of the program was launched on June 28, 2010, and can even read the Apple iPad (Fig. 2).

When we start using the tool, we first need to choose which type of acquisition we want to conduct – logical or physical. We start the tool after we plug the cable into a mobile device – in this case the Apple iPhone 3G (Fig. 3).

In our case, we have chosen the logical acquisition and we are presented with the following screen:

Fig. 2 Micro Systemation XRY

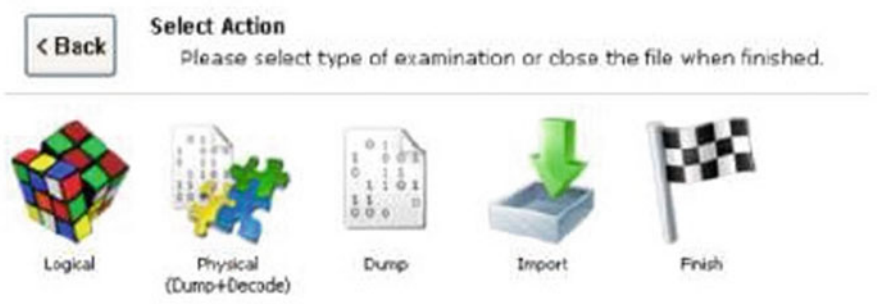


Fig. 3 Types of data acquisitions

Fig. 4 A logical acquisition

Figure 4 shows all kinds of data that will be collected with this tool and for this device. This can vary depending on the device we use. With a click on "Next" we start the process of data collection, which for this device will take about 30 min (Fig. 5).

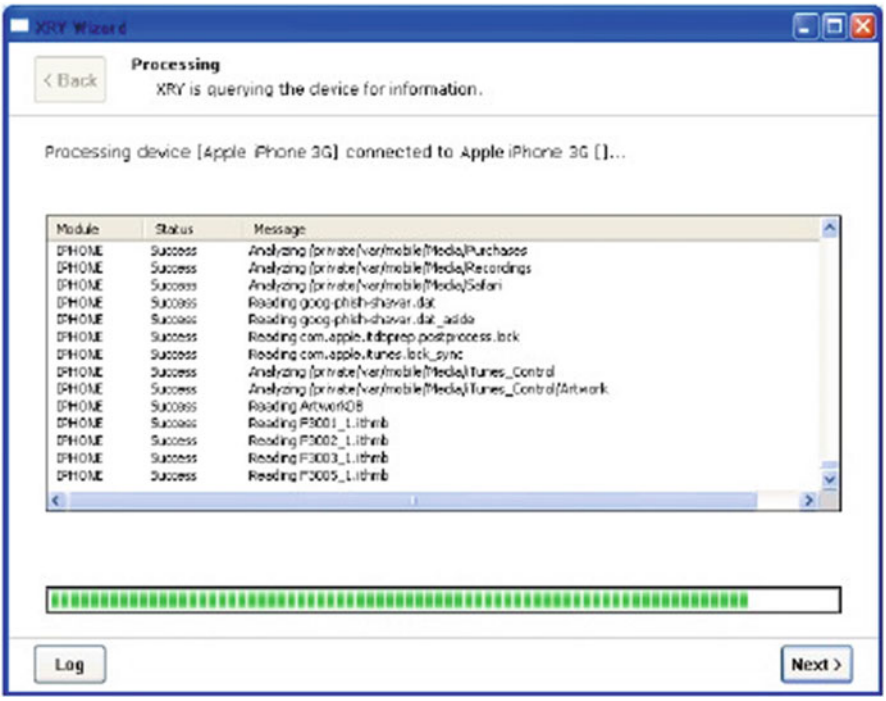


Fig. 5 The process of data collection

When the scanning and collection of the data have been completed, everything is stored onto an ".xry" file. Opening the file, we can see the report results, and the left side shows the data tree with following categories: Summary, Case Data, General Information, Contacts, Calls, Calendar, Notes, SMS, MMS, Pictures, Videos, Audio, Documents, Files, and Log. In the SMS and MMS, calls, and voice mail section, there is a tab called "deleted" at the end of each row. This is where the deleted data is stored.

With a click on "General information," we get to the next window which shows the main characteristics of the device (Fig. 6):

Going to different categories, the presented data changes. We get all kinds of information about contacts, especially for specifically chosen contacts on the right side of the window. Calls look similar to the call history on a phone, they present missed, received, and outgoing calls. This tool is one of the few tools to show deleted notes and all others read notes from the device. Other tools often just create a pretty unclear file (Fig. 7).

SMS messages from the phone can be acquired with all sorts of details (Fig. 8).

MMS messages are stored or can be directly accessed within the software. Pictures and video recordings are also stored into special categories and contain all files ever recorded with this camera, even those sent through MMS.

Fig. 6 General information

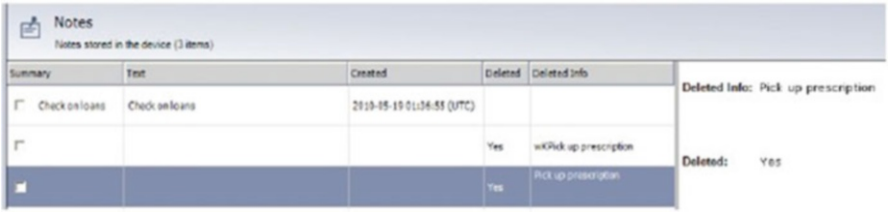


Fig. 7 Notes

Data for advanced users or data that can be more important for an investigation is stored in the log section. Inside this section you can find data about network access, internet search history, markers, investigations, accounts, etc.

Each data in this tool has its own index number and "home," which can be checked in order to show or not include the specific data set in the final report.

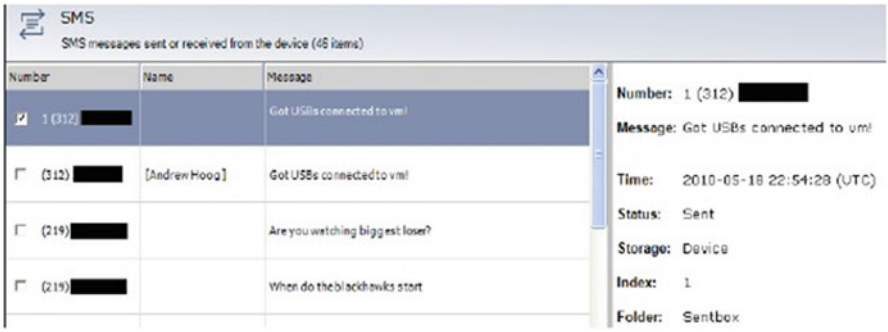


Fig. 8 SMS messages

Conclusion

The goal of mobile device forensics is to recover data (evidence) from mobile devices by using different methods, where each method has its own conditions. When these conditions are met, the problem of having collected invalid data is solved, and data that has been collected this way can be used as evidence in judicial proceedings and other processes. The practice has statistically shown that there are many cases where such data was the key evidence.

Mobile device forensics differ from desktop computer forensics, because mobile devices are working in different networks, which further impacts the process of delivery and keeping and processing the data. Apart from collecting data, mobile device forensics also values the connection between the process of collection and device hardware. This way, the user gets a feedback which gives him complete insight in the organization of the mobile device and the spectrum of his capabilities. All processes are being conducted step by step, which ensures more security and validity of the output results.

The way in which data is being collected from mobile devices can be different, depending on the type and condition of the device and can even be different if we take into account the condition of the data we're trying to recover.

Mobile device forensics, a type of forensics which falls under computer forensics, covers cell phones, smartphones, tablets, personal digital assistants (PDA), and GPS receivers. All of these fall under computer forensics. Because mobile devices are becoming more and more of an instrument, meta, or a recording tool for a crime, they have become an item of special interest in a criminal investigation, a civil lawsuit, or the collection of information data. Some even go so far as to claim that mobile devices contain more evidence per byte than traditional computers. Most smartphones now come with sophisticated apps and built in cameras, lots of storage capacity, and fast network connection, which leads to a great computing power being easily available for users. Despite mobile device forensics also taking into account eventual deleted data, in criminal or civil lawsuits, these processes are also used in

applications outside the court. Data that can be extracted from these devices includes call history, sent and received messages (SMS) and multimedia messages (MMS), contacts and phone numbers, emails, photos, video recordings, geographic and GPS information, network settings, web history, voice messages, social network information, application history, log files, and other data that can be found with smart applications.

References

Casey, E. (2004). *Digital evidence and computer crime: Forensic science, computers, and the Internet*. Amsterdam: Academic.

http://en.wikipedia.org/wiki/Boundary_Scan.

http://igorfranc.blogspot.com/2012/11/digitalna-forenzika-mobilnih-telefona-i.html. 29 May 2013.

http://www.datasolutions.rs/srp/spasavanje-podataka/spasavanje-podataka-sa-digitalnih-medija.html. Rescuing Data from digital Media 25 May 2013.

http://www.telekomunikacije.rs/aktuelni_broj/mr_igor_vukovic.html. 05 June 2013.

http://www.telekomunikacije.rs/aktuelni_broj/mr_igor_vukovic.html. 06 May 2013.

https://viaforensics.com/resources/white-papers/iphone-forensics/micro-systemation-xry/#forensic-acquisition. 10 June 2013.

Keonwoo, K., Hong, D., Chung, K., & Ryou, J.-C. (2013). *Data acquisition from cell phone using logical approach*.

Mokhonoana, P., & Oliver, M. (2007). *Acquisition of a Symbian smart phone's content with an on-phone forensic tool*. Information and Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria, South Africa.

Reyes, A., & Wiles, J. (2007). *The best damn cybercrime and digital forensics book period*. Rockland: Syngress.

Wang, Y., Streff, K., & Raman, S. (2012). Smartphone security challenges. *Computer – IEEE Computer Society, 45*, 52–58.

Willassen, S. (2005). Forensic analysis of mobile phone internal memory. Springer, Boston, USA.

Cyber War: Do We Have the Right Mindset? 38

Daniel F. Baltrusaits

Contents

Abstract

In security circles, an ongoing debate on the nature of war revolves around the influence of cyberspace. Many security experts warn of a cyber "Pearl Harbor" that has the potential to cripple critical infrastructure of a targeted state. However, the history of cyber attacks suggests that this warning is overstated and that political interests will limit the extent of operations in the cyber domain just as war in the terrestrial domain. Counter to predictions, given the heavy reliance on cyber capabilities by modern economies, instances of cyber war and cyber warfare are relatively rare. Cyber experts and intelligence officials seem to be inflating the threat when evaluating the national security threats from cyberspace.

D. F. Baltrusaits (✉)
National Defense College of the United Arab Emirates, Abu Dhabi, UAE

Near East South Asia Center for Strategic Studies, National Defense University, Washington, DC, USA
e-mail: daniel.baltrusaitis@ndc.ac.ae; d.f.baltrusaitis.ctr@ndu.edu

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_24

This chapter will analyze cyber war from a war theory perspective and show that by ignoring the political goals of state action, many cyber theorists and security experts fail to understand the political goals of a cyber operation and therefore overestimate the risk to a given threat. Although the cyber domain is unique, the threats from the domain do not fundamentally change the nature of war. Military forces can effectively plan and execute operations in cyberspace using the same strategy and doctrine already used in the physical domains. Thus, cyberspace operations can be part of the tools of national power already used by states to influence other states.

Keywords
Cyber attack · Cyber operations · Cyber security · Cyber war · Cyber warfare · Denial of service (DoS) · Distributed denial of service (DDoS) · Estonia · Georgia · Information warfare · International Atomic Energy Agency · Iran · Israel · Olympic Games · Russia · Stuxnet · United States · War theory

Introduction

In June 2010 testimony before the Senate Armed Service Committee, then U.-S. Director of Central Intelligence Leon Panetta stated, "the next Pearl Harbor that we confront could very well be a cyberattack that cripples America's electrical grid and its security and financial systems" (Bumiller and Shanker 2012). Five years later, in testimony to the same committee, the Director of National Intelligence warned, "Although we must be prepared for a catastrophic large-scale strike, a so-called cyber Armageddon, the reality is that we've been living with a constant and expanding barrage of cyberattacks for some time" (Bennett 2015). Clearly this scenario is frightening. According to cyber experts, the development of cyber capabilities by adversaries and non-state actors provide an unparalleled threat to state security due to the heavy reliance on the internet, low entry cost for actors willing to do harm, and high probability of damage to essential systems.

Richard Clark, former U.S. National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States under the Clinton and Bush administrations, and Robert Knake, former U.S. Director for Cybersecurity Policy at the National Security Council, outline the stark outcome possible for cyber war in *Cyber War: The Next Threat to National Security and What to Do About It* (2011):

> Several thousand Americans have already died, multiples of that number are injured and trying to get to hospitals. There is more going on, but the people who should be reporting to you can't get through. In the days ahead, cities will run out of food because of the train-system failures and jumbling of data at trucking and distribution centers. Power will not come back up because nuclear plants have gone into secure lockdown and many conventional plants have had their generators permanently damaged. High tension transmission lines on several key routes have caught fire and melted. Unable to get cash from ATMs or bank branches, some Americans will begin to loot stores. Police and emergency services will be overwhelmed.

Clearly the potential consequences of a full-scale cyber attack would be catastrophic.

According to the U.S. Department of Homeland Security (DHS), U.S. national critical infrastructure is vulnerable to cyber attack. In 2009, DHS marked 18 critical infrastructure sectors including essential services such as energy, water, transportation systems, communications, banking and finance, emergency services, and government services vulnerable to cyber attack. Unfortunately for national security, as much as 90 percent of U.S. critical infrastructure is owned by the private sector and vulnerable by varying degree to cyber attack (Department of Homeland Security 2009). Clearly, due to the reliance on the cyber domain for a large portion of critical infrastructure, security professionals must analyze and understand the consequences of a cyber attack that disrupts or destroys this infrastructure.

Amazingly, however, given the heavy reliance on cyber capabilities by modern economies, instances of cyber war and cyber warfare are relatively rare. Cyber experts and intelligence officials seem to be inflating the threat when evaluating the national security threats from cyberspace. A recent study by researchers Valeriano and Maness (2015) shows that from 2001 to 2011, rival states have engaged in only 111 cyber incidents within 45 larger cyber disputes. Additionally, the severity of these incidents has been relatively minor. A substantial number of attacks involved denial of service (DoS) and distributed denial of service (DDos) attacks that prevent legitimate users from using a service, but leave little long-term damage. For comparison, over a slightly shorter timeframe (2001–2010), there were over 1390 militarized incidents with a number involving fatalities (Palmer et al. 2015). Interestingly, this empirical evidence does not back claims that the cyber domain is rapidly becoming the new arena for international competition.

Cyber experts argue that barriers to entry are low and therefore change the dynamics of international interaction. Cyber capabilities in general are much cheaper than traditional weapons, and are therefore also accessible to a larger pool of state and non-state actors. These low barriers of entry enable a larger set of actors that complicate traditional balance of power models and erode powerful states' power (Weinstein 2014). If this is true, why do we not see more cyber war, especially from weak actors against great powers? This chapter aims to explain why.

Cyber War in Theory

Failing to conceptualize and understand the goals of a cyber attack skews theorizing on the potential uses of the cyber domain as a tool of state and non-state actors and results in faulty policy responses. While the use of cyber tools in peace and conflict is obvious, the theories of how and why they will be used are in debate. One important debate concerns the goals and magnitude of cyber war. Clearly, the warnings of Panetta, Clapper, Clarke, and Knake of destruction brought through the cyber domain are troubling; however, a look at war itself sheds light on the potential uses of cyber to affect a potential adversary.

Thomas Rid (2012), in his seminal article "Cyber War Will Not Take Place" largely argues that we must be concerned with precise language and that to be called cyber war "an offensive act has to meet certain criteria in order to qualify as an act of war. Any act of war has to have the potential to be lethal; it has to be instrumental; and it has to be political." Rid highlights a serious flaw in the current debate using theoretical arguments developed by nineteenth century military theorist Carl von Clausewitz. Rid argues that three features are an essential element of war's character. Quoting Clausewitz, Rid states, "All war, pretty simply, is violent. If an act is not potentially violent, it is not an act of war." Additionally war must be instrumental. It "has to be a means and an end. Physical violence or the threat of force is the means. The end is to force the enemy to accept the offender's will." Finally, an act of war must be political; "war's larger purpose is always a political purpose." According to Rid, cyber actions are unlikely to cross the threshold of war because no attack on record meets all of these criteria. Rather, he argues that we are seeing increasingly sophisticated acts of network-enabled sabotage, espionage, and subversion.

Josh Stone (2013) in "Cyber War Will Take Place!" counters that not only is cyber war possible but that it will take place. He argues, "the allegedly 'bloodless' character of cyber attacks is particularly challenging, because it demands that we think through the relationships between force, violence and lethality more systematically than has hitherto been done." According to Stone, violence is not an essential element in war, but rather the essential character is the political object. Cyber war is possible in the sense that cyber attacks could constitute acts of war. In his critique of Rid, he argues "acts of war involve the application of force in order to produce violent effects. These violent effects need not be lethal in character: they can break things, rather than kill people, and still fall under the rubric of war." In Stone's view, the definition of war is troubling rather than whether a true cyber war is possible.

Although these arguments seem semantic, they have important implications for decision-makers. One must ask the question "is cyber war possible and more importantly how will it manifest itself?" If the barriers to entry are so low, and attribution difficult as experts describe, why aren't minor actors waging an effective cyber war against greater powers today, and at what threshold would cyber actions reach the threshold of an armed response? If cyber war exists, then logically traditional war would remain an option in response. Therefore, policy makers should be asking themselves if cyber war is possible, how would it manifest itself and how does a state respond to this threat. To explore these questions I will also look to war theorist Carl von Clausewitz; however, I will use a broader analysis of his theory on war to give us insight into the questions posed above.

Prussian general and student of Napoleonic strategy, Carl von Clausewitz's (1989) *On War* is known in military and security circles as "the most profound, comprehensive, and systematic examination of war that has appeared to the present day" (Howard 1989). In this thoughtful work, Clausewitz is asking a very similar question to the one we face today in cyberspace; given the nature of war, why do belligerents not rapidly move to the maximum use of force? In Chap. 1, he develops this argument, "war is an act of force, and there is no logical limit to the application of that force." He continues, "Each side, therefore, compels its opponent to follow suit; a reciprocal

action is started which must lead, in theory to extremes." Given the assumption that a state in conflict does not want to lose, it would be compelled to use a maximum amount of force to ensure victory. However, this is rarely the case. Therefore, according to Clausewitz, there must be forces at work that "circumscribe" and "moderate" the extremes. Clausewitz would see the scenarios outlined above by Secretary Panetta and Director of National Intelligence Clapper as depictions of the extreme.

Clausewitz argues that war, as we know it, does not tend to the extremes for several reasons. First, war is never an isolated act. He states, "War never breaks out wholly unexpectedly, nor can it be spread instantaneously. . .Such shortcomings affect both sides alike and therefore constitute a moderating force." Second, war does not consist of a single short blow. The cyber Pearl Harbor reference illustrates this point. One party may try for a single strike that is so devastating that the other side submits to the will of the instigator, but "the very nature of war impedes the *simultaneous concentration of all forces* (emphasis in original)." Finally, in war the result is never final, "the defeated state often considers the outcome merely as a transitory evil, for which a remedy may still be found in political conditions at some later date." Given that the extreme is no longer feared or aimed for, war tends to be a matter of judgment on what degree of effort is necessary.

But how does the head of state determine the degree of effort? In the words of Clausewitz, "the political aim will reassert itself." The political motive for the war determines the military objective to be reached and the amount of effort it requires. This is not a simple calculus because once hostilities begin, passion can easily overrule reason (Echavarria 2007). It is important to note, however, that the political stakes largely determines the level of violence and effort. This brings us back to Thomas Rid's argument that cyber war is unlikely to happen because it is not violent. More importantly, cyber war is not likely to happen because it is neither violent, nor is the political object likely to be obtained through cyber action alone. An essential distinction that Clausewitz makes is that "war is not merely an act of policy but a true political instrument, a continuation of political intercourse, carried on with other means" (Clausewitz 1989). In other words, cyber war would have to be an act of policy that meets the political objectives of the initiating state.

In summary, for Clausewitz, the distinction that a war must meet the political objectives of the belligerents creates some problems for the concept of cyber war. The cyber war must meet a strategic objective; it needs to deter or compel an adversary to change its actions, and this is where cyber war as an independent entity becomes unlikely. To be an effective form of warfare, cyber war must fulfill the existing functions of conventional warfare if it is to rival the utility of existing forms of conflict (Gartzke 2013). A look at several case studies will illustrate these concepts.

Cyber War in Practice

Although alarmists warn that devastating and damaging cyber attacks are right around the corner, there are relatively few instances of cyber being used to advance national policy, and even fewer with positive results. Examples proffered of the

dangers of the new domain often include the Russian-sponsored cyber attacks against Estonia and Georgia, and the use of Stuxnet to degrade the Iran's uranium-enrichment capabilities. Unfortunately, for alarmist predictions, most of these events were relatively inconsequential for strategic decision-making and the effects were transient and low cost. A review of these conflicts will highlight the limitations of cyber as a coercive strategic tool.

Estonia 2007

Russian-sponsored cyber actions against Estonia in April 2007 and Georgia in 2008 are often listed as the first cases of cyber attack for political purposes. In both cases, alleged Russian hackers attacked government websites in a coordinated campaign in an effort to influence the decisions of the targeted country. In both cases, Russian hackers limited the ability of target governments to access and use information; however, the political effects were very limited and often contradictory to Russian interests.

In the spring of 2007, Estonia, a former Soviet Republic, became the target of a massive cyber attack against both government and private infrastructure. This attack was in response to parliament's decision to move a 6-foot-tall bronze soldier statue from downtown Tallinn, the capital, to a military cemetery a few kilometers away (Bronk 2016). This Soviet-built monument commemorated their war dead in driving Nazi Germany from the region. To many Estonians, the statue was a symbol of an oppressive Soviet occupation. The Russian government responded that Estonia would suffer serious consequences if it continued to move the statue (Davis 2007). In an apparent response to the move, Russian hackers activated a network of infected computers, or "bots," that were mobilized to overwhelm a government and private servers with requests for information and crash it – an attack known as distributed denial of service.

The Russian-sponsored attack remained relatively unnoticed until information technology (IT) managers noticed that website traffic was increasing to levels that would exceed their bandwidth allocations. Initial attacks were aimed to disable the Estonian press and government websites. The head of IT at *Postimees* (a local Estonian news outlet), Ago Väärsi, was able to mitigate the effects of the attack through managing the bandwidth of the website and coordinating for more bandwidth from their internet provider, but these solutions had limited effect. Eventually, traffic from overseas overwhelmed the paper. Väärsi had to block all international requests to the paper. This provided access to the paper again within Estonia, but in the eyes of the world, the paper disappeared (Davis 2007). This story was repeated across Estonia. By the end of the first week of the attack, users could no longer access most major Estonian papers, government websites, and Estonia's leading bank because distributed denial-of-service attacks had knocked the sites completely offline (Richards 2009).

Russian hackers, or hacktivists, were encouraged to hack Estonian sites through Russian-language chat rooms. First they were provoked by nationalist rhetoric about

the April 27 removal of the statue; a week later, they were encouraged to launch a massive attack at the stroke of midnight on May 9, the day Russia celebrates its World War II victory. At exactly 11 p.m. (midnight Moscow time), Estonia was slammed with a 200-fold surge in internet traffic. In a larger-scale version of what had happened to *Postimees*, nearly 1 million computers suddenly navigated to a multitude of Estonian sites, ranging from the foreign ministry to the major banks. Estonia's entire bandwidth capacity was being squeezed (Davis 2007).

By May 10, the cyber attacks forced Hansapank, the nation's largest bank and a leader in Estonian e-banking, to shut down its internet-based operations. The effects on banking were important for three reasons. First, online banking was disrupted in a country where an estimated 97 percent of all banking transactions occurred online. Second, it also severed the connection between Hansapank and its ATMs throughout Estonia. And third, it isolated Hansapank from the international banking system, thus preventing Estonian debit cards from working outside of the country (Richards 2009).

Over the course of 3 weeks, targeted websites grew to number in the hundreds as government pages, banking systems, news and media outlets, and sites of prominent Estonian universities were systematically attacked and shut down. The Estonian government was able to counter some of the effects of the DDoS attacks by tracing the Internet Protocol (IP) addresses of attacking computers and asking network operators to sever service from those addresses. In doing so, the government cut Estonia from the offending computers; however, this required significant effort tracking offending nets of attacking computers, many of which were insidiously tasked by Russian hackers (Richards 2009). This coordinated defense was somewhat successful, but what eventually brought normalcy back to Estonia was that the computer bots seemed to be programmed to attack for 2 weeks (Davis 2007). Estonian web traffic to target sites returned to a manageable load and on May 19, the attacks stopped as quickly as they started.

Estonian authorities were able to watch coordination for the attack on Russian-language websites and later traced some of the attacks to Russian Internet Protocol addresses. Given that these attacks were coordinated and emanated from Russian territory, Estonian authorities believed the attacks came from the Russian government, and Estonian Defense Minister Jaak Aaviksoo contacted the North Atlantic Treaty Organization to see if they could obtain military assistance under Article V (Brenner 2009). While NATO did not consider the cyber attack reaching the level of armed attack under Article V, it did react quickly by sending several key cyber experts into the country to assess the situation and assist Estonia's Computer Emergency Response Team (CERT) to assist in limiting the damage by the attacks (Richards 2009).

The immediate implication of the DDoS attacks for Estonia was the loss of services for government, communication, and banking in one of the most internet-connected countries in the world. Hansapank, one of the main financial targets, suffered economic losses estimated at $1 million (Kozlowski 2014); however, shortly after the incident, Swedbank group voted to discontinue the Hansapank brand and all operations were rebranded under the Swedbank name (Katznelson

2013). Although the effects were massive during the incident, quick action by Estonia's CERT, NATO, and the international community minimized the effects of the attack. There was no permanent damage to the information technology infrastructure and financial losses were minimal.

The Russian government vehemently denied any involvement in the attacks; however, circumstantial evidence supports the perception that the Russian government was behind or at a minimum supported the cyber attacks. The Russian government repeatedly denied directing or participating in the attacks, but also refused Estonia's diplomatic request to help trace the attackers (Clarke and Knake 2011; Springer 2015). Substantial evidence demonstrated that the attack was orchestrated in Russian chat rooms and the botnet controllers were in Russia. The government argued that the attack was the work of Russian patriots rather than a government-controlled effort; however, the high level of coordination on the attacks suggests that the government was at least a tacit sponsor (Springer 2015).

From a Clausewitzian perspective, the cyber attacks did not meet Russian political objectives and in many ways ensured that Estonia moved closer to NATO. The Estonian attacks did demonstrate that state actors might attempt to disrupt government and commercial IT infrastructure as a signal short of military action; however, the strategic results were minimal strategically (Bronk 2016). Russia's goal was to maintain a higher presence in Estonia by influencing Estonia's Russian-speaking population through national symbols on Estonian territory. In the wake of the statue's move, both houses of the Russian parliament called on Russian president, Vladimir V. Putin, to impose sanctions on Estonia or sever relations with the country. The Russian foreign minister, Sergey V. Lavrov, stated, "This is blasphemous, and will have serious consequences for our relations with Estonia" (Myers 2007). The cyber attack seemed part of a more elaborate campaign to influence Estonia, since it took other low-level actions to sanction the Estonians. Although no official sanctions were announced, Russia claimed the need to repair to railway lines to restrict oil and coal exports through Estonian ports in early May 2007 (Wagstyl 2007). Estonia did seem to suffer some short-term reduction in port and rail activity, but it quickly recovered (Pukk 2011). Overall, Russian political outcomes for Estonia remained unmet after the attacks. The Bronze Night was still moved to a less prominent location, although the Estonian authorities ensured that it was maintained and given more prominence. As an unintended consequence, NATO created a cyber defense center in Estonia in 2008, the presence of which is intended to show NATO's resolve to defend against cyber and physical attacks (Clarke and Knake 2011; Springer 2015). The Estonian attacks highlighted to the government vulnerabilities in e-government interaction with constituents and has strengthened its ability and resolve to counter a similar use for coercion.

Georgia 2008

A year after the Estonian cyber attack, the Russian government again was implicated in using cyber attacks against another post-Soviet Republic. In 2008, Russian

military forces, supported by cyber attacks, invaded Georgian territory to support pro-Russian independence movements in South Ossetia and Abkhazia. The Russian military campaign marks the first instance of overt cyber attacks being integrated with traditional military operations (Bonner 2014). According to one researcher, "This appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains" (Hollis 2011). This episode is important because it clearly shows the use of cyber tools to directly affect a military campaign, and therefore meets Clausewitz's definition of the use of violence to gain a political effect.

Following Georgian independence from the Soviet Union in 1991, Russian nationalists in the provinces of Abkhazia and South Ossetia fought with the newly formed Georgian state to secede from the country. Simmering tensions resulted in full-scale conflict with Georgia in both regions. Both conflicts ended with negotiated settlements reached in 1992 and 1994, respectively, forming autonomous regions where Georgia maintained little control. The violence subsided with ceasefire agreements; however, the root conflict remained unresolved and sparked the Russian intervention in 2008 (Bonner 2014). In early March 2008, Abkhazia and South Ossetia submitted requests for their recognition to Russia's parliament in response to the West's recognition of Kosovo. Russian President Vladimir Putin did not rush to recognize Abkhazia and South Ossetia but rather used the conflict as a tool to check NATO expansion in Georgia (Associated Press 2008). Tensions continued to escalate during spring and early summer when Russia unilaterally deployed further troops and moved heavy artillery into Abkhazia under the auspices of a CIS-sanctioned peacekeeping mission (European Parliament 2008). On August 1, South Ossetian separatists began shelling Georgian villages, with a sporadic response from Georgian peacekeepers in the region. To put an end to these deadly attacks and restore order, the Georgian Army was sent to the South Ossetian conflict zone on August 7.

Moscow accused Georgia of "aggression against South Ossetia" and responded by immediately deploying troops to South Ossetia, initiating bombing raids on Georgia, blockading the Georgian Black Sea coast and landing marines on the coast of Abkhazia. Russian and South Ossetian forces combated Georgian military forces in and around South Ossetia for several days, until Georgian forces retreated. The Georgians were outmatched by the Russian intervention and were forced to retreat to protect the capital of Tbilisi. After 5 days of fighting, French President Nicolas Sarkozy, acting on behalf of the European Union, negotiated a ceasefire agreement on 12 August 2008 between Russian President Dmitry Medvedev and Georgian President Mikheil Saakashvili (Tagliavini 2009b). Moscow agreed to exit occupied territory once an international peacekeeping force arrived. The force never materialized and shortly Russia recognized Abkhazia and South Ossetia as independent states. The states then asked Russian forces to remain (Clarke and Knake 2011).

In the midst of this significant military intervention, Russia also engaged in cyber activity against a wide range of Georgian government and commercial assets. The attack is noteworthy in that it is the first known instance of overt cyber attacks being incorporated into a conventional military campaign. A dry run of the initial cyber

attack started weeks before military operations. On July 20, 2008, the website of the Georgian president came under a DoS cyber attack. Security researchers in the United States noticed a barrage of DoS attacks that overloaded and effectively shut down Georgian servers including a data stream containing the message: "win+love +in+Rusia." According to technical experts, the attack appeared to be a dress rehearsal for the larger effort when shooting started (Markoff 2008). A similar scenario with attacks on a larger scale coincided with Russian troops entering South Ossetia.

The Russian cyber attack was carried out in two phases. In the first phase of attack, hackers focused mainly on Georgian news and government websites using botnets to conduct primarily brute DDoS attacks. This seemed to be an effort to disable Georgian ability to determine the scope and nature of the Russian conventional military operations. According to U.S. Cyber Consequences Unit (US-CCU) analysis, the initial cyber attacks were clearly designed to make it harder for the Georgians to determine what was happening in the restive areas (Bumgarner 2009). The cyber attacks were sophisticated in their targeting, in that botnet assault was focused on 11 targets that were consistently targeted throughout the conflict (Bonner 2014). According to cyber experts, the defacement and denial campaign disrupted the ability of the Georgian government to understand the scope of the invasion and disseminate information to the public. Communication between business executives, journalists, community leaders, and government officials was impeded during the cyber campaign because sources of information and general communications were jammed (Bumgarner 2009).

Georgia's first reaction to the cyber attack was to contact Estonian officials, who had managed the 2007 cyber attacks. These officials put the Georgians in touch with an informal network of international cyber-security experts who were able to offer help and advice (Bumgarner 2009). Much like their Estonian colleagues, Georgian IT managers attempted to counter the cyber attacks by filtering out messages originating from IP addresses in Russia. However, the cyber attackers quickly used either false IP addresses or routed their assault through foreign countries to counter Georgia's cyber defense filters (Bonner 2014). Foreign servers were used by Tblisi to stem the tide of attacks against government servers. Initially, Google's BlogSpot and European governments agreed to take over hosting websites of the Georgian government. Network administrators in Germany were able to temporarily reroute some Georgian internet traffic directly to servers run by Deutsche Telekom and the Ministry of Foreign Affairs built a replacement website to communicate on BlogSpot (Swaine 2008). Capability was eventually moved to US-based servers to counter the Russian hacking attempts. During the attacks of August 8, Tulip Systems, a private web-hosting firm in the United States owned by Georgian-born Nino Doijasvili, contacted Georgian government officials and offered assistance in hosting their internet capability in the US, apparently without US government approval. A day later, the Georgian government transferred attacked websites to hosting by Tulip Systems, including the websites of the Georgian President and the Ministry of Defense to protect them from malicious traffic (Korns and Kastenberg 2009; Russell 2014). Learning the lessons of the Estonian attacks,

Georgia relocated strategic cyber capabilities outside of its territory ensuring continued wartime communication with supporting governments, Georgian citizens, and military forces.

The second phase of cyber attacks expanded in scope and sector to include financial institutions, businesses, educational institutions, Western media, and a Georgian hackers website; however, hackers did not attempt to disrupt essential services that could have had a catastrophic effect on Georgian society. Russian hackers did not attempt to cripple critical infrastructure such as the Baku-Ceyhan oil pipeline through its SCADA network. These type attacks could have caused chaos or injury but hackers chose attacks that could trigger comparative inconvenience rather than consequence (Bumgarner 2009). Beside the DDoS attack, the hackers also instituted massive spamming of public email in order to disrupt e-mail communication (Kozlowski 2014). Hackers defaced websites of several prominent banks on August 9 leading the National Bank of Georgia to order all banks to discontinue electronic services and transactions. Service was restored on August 18 resulting in a 10-day disruption of electronic banking services (Russell 2014; Tikk et al. 2008).

Although cyber activity is difficult to attribute, the attacks once again showed a high degree of cooperation between Russian government and Russian hacktivist activity. Before the 2008 Russian attack on Georgia, "any civilian, Russian born or otherwise, aspiring to be a cyber warrior was able to visit pro-Russia websites to download the software and instructions necessary to launch denial of service attacks on Georgia" (Nye 2010). Cyber attacks against targeted Georgian government and news portals were coordinated in time and space with the corresponding military operations suggesting that there had to be close cooperation between the Russian military and the civilian cyber attackers.

Project Grey Goose, one of the most comprehensive investigations of the cyber attacks in Georgia, concluded that cooperation between the government and hacking groups was likely for several reasons. First, initial attacks were well focused and did not show any reconnaissance or mapping, but jumped directly to techniques that were best suited to jamming the websites under attack. According to cyber experts, this behavior indicates that the necessary reconnaissance and the writing of attack scripts had to have been done in advance. Second, given the speed of action, the signal to go ahead also had to have been sent before the news media and general public were aware of military activity in Georgia. Third, one of the main coordination websites, StopGeorgia.ru, was physically located in an apartment building next to a Russian Ministry of Defense research institute called the Center for Research of Military Strength of Foreign Countries. This facility is very close also to the headquarters of the foreign military intelligence directorate of the General Staff of the Armed Forces (GRU). Finally, the fact that Russian hackers did not carry out physically destructive cyber attacks against Georgian critical infrastructure industries suggests coordination with and restraint directed by the Russian government (Bumgarner 2009; Russell 2014).

In the end, the effects of the cyber attacks had much less influence on Georgian strategic decision-making than cyber experts claim. Although experts claim that

cyber attacks kept the government from communicating with the local population, limited the government's ability to spread its message online, and to connect with sympathizers around the world during the fighting with Russia, this claim seems specious. First, Georgia was a relative latecomer to the internet and only seven percent of the population used the internet daily (Bonner 2014); therefore, the population was unlikely to look to the internet for news. At the local level, government websites were not the important means of communication with the population (especially outside of the capital) and TV outlets were primary means for reaching out to wider public throughout the war (Mgaloblishvili 2017). The government was able to effectively communicate with alternate internet providers, the US and European governments, and the international news media. Although the effects seemed significant at the time, Georgia saw little effect beyond inaccessibility to many of its government websites (Markoff 2008). Finally, Georgian decision-makers claim that the cyber attacks had little effect on information gathering or decision-making. Quick Russian victories in South Ossetia and Abkhazia had more to do with outmatched Russian conventional capability rather than information advantage. Russia's military was able to overpower and scare off the inexperienced Georgian Army with force 25,000–30,000 Russian troops, almost as large as the entire Georgian military (Chivers and Shanker 2008; Tagliavini 2009a). According to Georgia's Ambassador to Turkey Grigol Mgaloblishvili (2017), who had a key role in the crisis response during the attack, "the cyber attacks had zero influence on strategic decision-making given the scope of Russian conventional military operations and their threat to the capital of Tbilisi." Overall, although cyber capabilities enhanced the Russian invasion, the short- and long-term impact on Georgia was limited.

Politically, cyber operations were partially successful, in that the timing of the cyber attacks coincided with the ground assault causing some confusion at the local level. However, senior leaders state that the actions did not limit access to critical information and interactions with foreign leaders progressed normally. Russian leaders, however, believe that the operation did meet their objectives and consider Georgia a learning laboratory for integrating cyber operations and information warfare with military attack. According to Russian Chief of General Staff Valeriy Gerasimov, the role of military operation in obtaining political goals has changed. According to Gerasimov, the goal is now "achieving political goals with the minimum armed impact on an adversary. Predominantly by undermining his military and economic potential, by applying informational and psychological pressure…" (Giles 2016). The operation in Georgia, however, still failed to meet Russian primary objectives in Georgia. Cyber activity merely sowed low-level confusion rather than enabling strategic effects outlined in Russian documents. Unlike the predictions outlined earlier, cyber was not used to replace the use of force in conflict, but rather to work in coordination with the use of military power and in this case had limited effect. If cyber attack was a more effective tool of national power, Georgia would be expected to use its cyber capability rather than conventional military force. Terrestrial military force was the logical choice for claiming contested territory in Abkhazia and South Ossetia.

Stuxnet

The 2010 Stuxnet virus displayed a marked increase of sophistication compared to the Russian attacks and ushered in a new era of computer network attack (CNA). A joint US–Israeli component of a broader US cyber campaign against Iran code-named *Olympic Games*, the Stuxnet worm disrupted Iranian nuclear enrichment by infiltrating and damaging centrifuges run by computers in the Natanz nuclear complex (Nakashima and Warrick 2012). The goal of *Olympic Games* was to retard Iran's progress in developing nuclear weapons without the danger of a physical military attack on Tehran's nuclear infrastructure (Farwell and Rohozinski 2012). Stuxnet demonstrated that a computer network attack could cause physical damage across international boundaries and was the first-known instance of remote control warfare over the internet that could be the harbinger of the cyber Pearl Harbor. The attack was credited with damaging over a 1000 centrifuges at the Natanz uranium-enrichment facility and according to senior Mossad official delayed acquisition of a nuclear device up to 5 years (Lindsay 2013).

Iran's nuclear program generated international concern when in August 2002 the National Council of Resistance of Iran revealed the existence of undeclared nuclear facilities in Iran that included enrichment facilities in the Natanz Enrichment Complex, as well as potential weaponizing activities in a heavy water production facility at Arak. Despite intensive investigations by the International Atomic Energy Agency (IAEA) and intense diplomatic pressure, including the passage of several United Nations Security Council Resolutions (UNSCRs) and multiple sets of UN sanctions, Tehran continued to engage in enrichment activity that had no credible civil rationale because the Bushehr nuclear power plant used Russian fuel (Nuclear Threat Initiative 2016).

The international community, especially the US, was concerned with the development of indigenous enrichment capability that could be used to weaponize uranium. Gas centrifuges enrich uranium by spinning uranium hexafluoride gas at high speeds to increase the concentration of the uranium-235 isotope. These centrifuges can produce both low-enriched uranium (LEU), which can be used in nuclear power reactors, but for which Iran had no known need, and highly enriched uranium (HEU), which is one of the two types of fissile material used in nuclear weapons. Tehran claimed that it wanted to produce LEU for its current and future power reactors; however, those claims are not credible since Russian-supplied fuel is intended to power its reactors at Bushehr (Bowen and Brewer 2011).

In 2002, the IAEA began investigating the allegations that Iran had conducted clandestine nuclear activities at Natanz, a remote facility 150 miles south of Tehran. After more than 3 years of investigation, the IAEA reported that some Iranian activities had violated Tehran's safeguards agreement. The IAEA Board of Governors referred the matter to the UN Security Council in February 2006 (Kerr 2016). The UN Security Council, through a series of resolutions since 2006, demanded that Iran suspend "its enrichment related activities" and its "work on all heavy water related projects." Iran continued producing low-enriched uranium (LEU) using first-generation IR-1 gas centrifuges that were Iran illicitly acquired from the A. Q. Khan proliferation network. This effort is troubling given that 72% of the effort to produce

weapons-grade HEU is accomplished by the time uranium is enriched to the LEU level (3.5%), and the same centrifuge cascades are capable of producing HEU (Bowen and Brewer 2011).

The Bush administration started to look at proposals for disabling Iranian enrichment capability in 2006 and started developing a cyber capability code, named *Olympic Games*, to sabotage the production means as an option rather than conventional coercive options. Stuxnet is believed to be one program developed under the $300 million *Olympic Games* umbrella (Bussing 2013; Valeriano and Maness 2015). By mid-2009, the Iranians had installed about 8000 centrifuges in one hall at Natanz. Destruction of this underground facility by direct airstrike would have been feasible, but it would have required a much larger and more sophisticated attack than the Israeli strikes at Osirak and Syria (Lindsay 2013). US strategic planners thus developed alternate, less-provocative, means to delay enrichment and to persuade Israel from launching airstrikes of its own.

President Obama secretly ordered a series of increasingly sophisticated attacks from the *Olympic Games* program on the integrated computer systems that run Iran's main nuclear-enrichment facilities. The initial attack began years before the Stuxnet attack with the insertion of computer code called a beacon to draw an electrical blueprint of Natanz's networks. Eventually, the beacon would "phone home" to the headquarters of the US National Security Agency with the structure and daily rhythms of the enrichment plant to understand how the facility's computers controlled the centrifuges used to enrich uranium. Getting the worm into Natanz required the US and Israel to rely on traditional spy craft to entice engineers or maintenance workers with physical access to the plant to insert thumb drives into targeted computers since the Iranians had isolated the enrichment network from the internet with an "air gap." These thumb drives were critical in spreading the first variants of the computer worm (Sanger 2012).

While developing the electronic map of the facility, the two countries developed a complex worm that the Americans called "the bug" to embed in the industrial control system (ICS) from Siemens used to control the Iranian centrifuges. The popular Siemens SIMATIC STEP 7 software ran on computers using Microsoft Windows operating systems and provided control and displays to monitor and control the centrifuge rotors (Lindsay 2013). The bug, now known as Stuxnet, targeted Microsoft Windows machines and networks and sought out the SIMATIC software and compromised the programmable logic controllers (Kushner 2013). To modify the SIMATIC software, an attacker would have to penetrate through components from multiple vendors and several concentric layers of defenses (Sanger 2012). Stuxnet was designed to replicate itself through a network while remaining undetected. It could travel through multiple pathways by removable media or through shared network resources like print servers. Hiding and encrypting its files along the way, the worm was able to vary its behavior depending on the antivirus software it encountered. Much like the beacon software, Stuxnet was designed to penetrate through firewalls and into computers that would have no direct connections to the internet. Stuxnet also could relay commands via a peer-to-peer network to allow remote command and control (Lindsay 2013).

To be sure of a reasonable chance of success, the bug needed testing. So, under enormous secrecy, the United States built replicas of Iran's P-1 centrifuges to mimic the design that Iran purchased on the black market from Khan, then built a functional replica of Natanz spread over several Energy Department laboratories to avoid suspicion. Military and intelligence officials then conducted destructive testing to determine if the bug would work. After several false starts, the tests were surprisingly successful. As designed, the worm invaded the target computers, sat dormant for days or weeks, then sent instructions to manipulate the speed of the centrifuges, ultimately damaging them by spinning at supersonic speeds (Sanger 2012).

Lacking other suitable options, President Bush in 2008 approved the use of Stuxnet to sabotage the Natanz enrichment operations. Like the earlier beacon, an Israeli proxy used a corrupt memory stick to install the Stuxnet virus (Sale 2012). The first attacks were small. Stuxnet's attack code instructed the centrifuge controllers to speed up near max speed for 15 min, then return to normal speed for 27 days, then slow down too slow to enrich for 50 min, and then finally return back to normal for 27 days. The worm's 2-month loop sped up and slowed the centrifuges to introduce chronic fatigue in the cascades rather than to simply break them in one violent shock (Lindsay 2013). When it attacked, the worm hid its actions by sending signals to the Natanz control room indicating that everything was operating normally. According to the IAEA, the Iranians had grown so distrustful of their own instruments and scientists that they had assigned people to sit in the plant and radio back what they saw. The centrifuges failed the engineers would close down whole loops of 164 centrifuges, looking for signs of sabotage in all of them. According to US intelligence intercepts, the Iranians were mystified about the cause (Sanger 2012).

When president Obama got to office, he authorized the attacks to continue. According to senior administration officials, his strategy was to use diplomacy, sanctions, and cyber attacks to continue slowing the Iranian program, but in 2010, an update of the code to speed up the attacks caused it to spread outside of Natanz, ultimately exposing the covert cyber program.

Stuxnet's operators modified the malware's code in the spring of 2010, to make the worm spread more aggressively (Albright et al. 2011). An error in the code allowed it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the internet, the bug failed to recognize that it was outside Natanz and continued to replicate itself. A programming error in the attempt to focus the effects at Natanz had allowed the virus to replicate itself "in the wild" where computer security experts could dissect it and figure out its purpose (Sanger 2012). Researchers at Kaspersky Labs and other security firms were able to reverse engineer the code highlighting to the public the number of infections, the fraction of infections in Iran, and the references to Siemens industrial programs, which are used at power plants. Kaspersky analysis showed that Stuxnet had been specifically designed to subvert Siemens systems running centrifuges in Iran's nuclear-enrichment program (Kushner 2013). Since it was unclear how much the Iranians knew about the now exposed code, Obama authorized the attacks to accelerate (Sanger 2012).

The results of the Stuxnet attack are mixed. By early 2010, Stuxnet destroyed about 1000 IR-1 centrifuges out of about 9000 deployed at the site. However, during this

period, Iran kept another 5000 centrifuges in stock, ready to be commissioned. Overall, the physical impact on operations seems limited. According to IAEA records, the IR-1 would fail at about a 10% rate; therefore, Stuxnet seemed to double that rate. However, even with the increased failure rate, Stuxnet did not lower the production of LEU during 2010. The physiological effect of this attack was much more significant. It rattled the Iranians, who were unlikely to know what caused the breakage, delayed the expected expansion of the plant, and further consumed a limited supply of centrifuges to replace those destroyed (Albright et al. 2011). Internal Obama administration intelligence estimates say the effort was set back by 18 months to 2 years. However, considering that enrichment levels recovered quickly, some experts estimate that Iran had developed enough fuel for five or more weapons (Sanger 2012).

The use of Stuxnet to delay Iran's nuclear program does meet a Clausewitzian definition of a political objective. Politically, the virus got some of the same results as using military force. The cyber program delayed production long enough to allow punishing sanctions and international pressure through the UN Security Council to pressure Iran to come to a negotiated settlement (Farwell and Rohozinski 2012). Importantly, it delayed the Iranian development program, induced uncertainty in the minds of Iranian leaders on the effectiveness of their technology, and provided the needed space for a negotiated settlement. Additionally, it allowed the US to manage a key strategic partner, Israel. By allegedly partnering with Israel, the US was able to de-escalate the conflict by giving Israel a strategic option other than a physical strike on Iranian facilities similar to their strikes at Osirak and Deir ez-Zor in Syria. Interestingly, however, the attack fell well short of a type of physical attack in comparison with the two earlier Israeli attacks in the region. The Obama administration specifically limited physical damage at Natanz so that the Iranian's would not suspect outside intervention (Gartzke 2013; Rid 2012; Valeriano and Maness 2015). The US could have written code to spin the centrifuges to immediate failure which likely would have damaged more equipment; however, this option would have exposed the cyber attack objectives much sooner and allowed the Iranians to develop effective countermeasures by isolating their industrial control networks.

Mirroring the arguments of Thomas Rid (2012), Erik Gartzke (2013), and Jon Lindsay (2013) on the Stuxnet episode shows that cyber tools are a much more important tool of state reconnaissance and espionage to be used in situations where conventional weapons are effective. From a policy standpoint, state and non-state actors gain an incredible edge by staying unnoticed in the cyber world and are therefore hesitant to show the scope of their capabilities. In the Natanz case, the Bush and Obama administrations both thought that a covert presence was more important than the effect of tipping their hand with a large destruction of centrifuges.

Limitations of Cyber Weapons

A Clausewitzian analysis of cyber conflict shows that the dangers of a full-blown cyber war are very unlikely. It must fulfill the existing functions of traditional warfare if it is to rival the utility of existing forms of conflict. Cyber attacks can be

appealing as political acts only to the degree that they affect the decisions that organizations and sovereigns make with and without cyber violence. Damage that can be quickly or easily undone will not do much to deter or compel, but it will alert an enemy to vulnerabilities in its defenses, and certainly also antagonize an opponent, increasing the risk of counterattack and general hostility (Gartzke 2013).

Cyber effectiveness will be limited for several reasons that generate restraint by policy-makers. First, what the unique ICS attack payload actually shows is that precision-targeted effects carry formidable requirements for specific intelligence and engineering expertise (Farwell and Rohozinski 2012). Other than denial of service attacks, there is no general-purpose software package for offensive cyber operations. Each application requires a significant reconnaissance and engineering effort to understand how targeted computer networks control key processes. The *Olympic Games* operation was so complicated that there could be no guarantee of success unless it was tested prior to the injection of the software. The mock centrifuge array used built by the U.S. Department of Energy required extensive state resources and capabilities (Valeriano and Maness 2015). To stay undetected, the Stuxnet code required an extensive knowledge of Natanz structure and processes. Stuxnet code details match exactly the details known about Natanz from IAEA inspections. The code specifically code defined arrays of 164 items organized into 15 irregular groups, which exactly matched the Natanz configuration of 15 enrichment stages in a cascade of 164 centrifuges (Lindsay 2013). In short, development of an effective worm required extensive knowledge of the operations of Natanz that were possible only by state-level organizations that had ample access to nuclear physicists, IAEA inspectors, experts on Pakistani developed centrifuges, and the intelligence assets to understand the physical and computer configuration at Natanz.

The second limiting factor is that highly developed viruses like Stuxnet are one-time use capability. Cyber experts estimate that the engineering effort for Stuxnet cost $300 million and probably took a team of 10 coders 2–3 years to develop (Kushner 2013). The edge given to the US and Israel for this large engineering effort was very transitory. Once the code was discovered, Stuxnet was easy to detect, reverse engineer, and defend from. Stuxnet was easy to dissect because it kept a history of the compromised machines, including name, domain name, and IP-address, in its body. The data was used for control purpose, but allowed Kaspersky Labs to track down the origin and characteristics of the virus, essentially giving cyber community the code and methods to counter it. According to Jeffrey Carr, the founder and CEO of Taia Global, a security firm in McLean, VA, "Whoever spent millions of dollars on Stuxnet, Flame, Duqu, and so on—all that money is sort of wasted. That malware is now out in the public spaces and can be reverse engineered" (Kushner 2013). Stuxnet performed four zero-day exploits, which was unheard of for a malicious worm, but once the code was analyzed and patches for software developed, these exploits are no longer useful. Once the code is understood, defenders can easily increase the resilience of their industrial control systems (Lindsay 2013).

A third limiting factor is the repurposing of code by other actors for malicious purposes outside the scope of the original attack. Although the effects of Stuxnet

were well targeted to the Natanz complex, the code has been detected on industrial control computers worldwide. Stuxnet also provided a useful blueprint to future attackers by highlighting the road to infiltration of hard targets. The Iranian facilities were thought relatively invulnerable because they were not connected to the internet. The Indian Ministry of Communications and Information Technology initiated a cyber attack crisis management plan after a senior official of a commercial power provider's IT department revealed that a Stuxnet type of virus originating from China attacked one of the routers in the power sector. Other India security experts claim that China reformulated Stuxnet to target India's space program, destroying India's INSAT-4B (Patel 2011). The implications of Flame and Stuxnet go beyond state-sponsored cyber attacks. According to a Symantic researcher, "Regular cyber-criminals look at something that Stuxnet is doing and say, that's a great idea, let's copy that" (Kushner 2013). Once released and reverse engineered, the original developer of computer attack tools no longer have control of uses by other actors; therefore, they will be hesitant to release code in the first place due to the danger that it places toward home country systems.

The fourth limitation is that the effects are temporary indicating that cyber is a weak tool of state interaction. Shutting down power grids, closing airports, or derailing communication could be tremendously costly in the short run, but most damage of this type will be fixed quickly and at comparatively modest investment of tangible resources. The three case studies presented in this chapter show that the physical effects and political consequences were limited. The most successful cyber attack, Stuxnet, still had limited influence in bringing Iran's nuclear program back under IAEA supervision. Much more effective tools were the economic sanctions on the regime. The computer actions had some effect, however, in building time for the economic sanctions to work.

Finally, in contradiction to the claim that cyber attack is a tool of the weak, the potential for blowback is high, especially when weak actors attack strong actors. Offensive cyber capabilities are rarely used because they could lead directly to war, or civilian harm. In short, states risk a response by the target state. The response can easily spread a conflict from the cyber realm to the physical world. This generates a self-limiting response that Valeriano and Maness (2015) describe as *cyber straitjacketing*. States and non-state actors limit the scope and intensity of cyber attacks based on the calculation of what they can get away with. Cyber actors rarely reach the level of attack that would generate a robust response due to the potential for harm. At a minimum, a cyber action highlights to a target the need for increased cyber defense making future interactions more difficult. Revealing a given set of cyber capabilities heavily degrades their usefulness in the future. Threatening the capacity to harm via the internet as a deterrent or compellent threat also means tipping the target off to vulnerabilities that can be remedied or compensated for, while inflicting harm seldom has a durable effect on the balance of power. This perishable nature of offensive cyber capabilities means that deterrent or compellent threats are time bound and thus creates little leverage for states that do not have the resources to invest heavily in offensive cyber assets (Gartzke 2013). Offensive cyber advantages being "use and lose" capabilities lose their value once threatened.

Conclusion: Cyber War Is Unlikely but Cyber Warfare Is Here

Clearly, policy makers need the proper mindset when discussing the use of cyber operations in conflict. Cyber attacks in isolation, or cyber war, have been relatively ineffective, but used in coordination with other tools of state power gives policy makers another tool to affect an adversary's decisions. According to noted cyber scholar Martin Libicki (2014), cyber war "is undertaken to affect the will of the adversary directly." The use of military force has been the tool of state power to affect an adversary's will directly. Typically, force is used to punish or compel an adversary to do something that it would not otherwise do. Or threats of force are used to increase the price of aggression therefore affecting adversary decision-making. Finally, force can be used directly to capture and control territory and thereby directly influence an adversary's actions (Gartzke 2013; Johnson et al. 2003). Cyber war is a weak tool of state power, in that it cannot capture territory and is unlikely to disarm or threaten an adversary sufficiently to change decision-making in areas of vital interest. The coercive effect of cyber war is weak since the threatened cyber capability has to be strong enough so that the defender is capable of being coerced. Cyber warfare – cyber attacks that are authorized by state actors against cyber infrastructure in conjunction with a government campaign – however when used with other instruments of national power can be used to positive effect and are likely to be seen in the future.

Brett Williams, the former director of operations for U.S. Cyber Command, captures the view that overemphasizing cyber war is a distraction from the time-honored principles of state interaction. According to Williams (2014), "War, conflict, and competition are all characterized by enduring principles that were established long before cyberspace." Focusing intently on the unique nature of cyber war results in a tendency to overstate the relevance of cyber warfare within the context of all other activities that influence a reacting adversary. The creation of cyberspace has simply offered another environment or domain within which to exercise the elements of national power. Cyber warfare then is as an important adjunct rather than an overwhelming weapon in inter-state wars.

The case studies in this chapter show that cyber attack has been used as a state tool to attempt to influence decision-making of an adversary. Russia, using networks of criminal hackers and hacktivists encouraged the government, used tools like DDoS attacks to create an atmosphere of uncertainty in Estonia and Georgia. They have used these attacks to amplify the Clausewitzian "fog" and "friction" inherent in conflict. Clausewitz noted that actual war is not like war on paper in that the fog – is the uncertainty in situational awareness experienced by participants; while friction – is the countless minor incidents that lower the general level of performance (Clausewitz 1989). Clearly, cyber tools have a role in influencing the decision cycle of an adversary. Current Russian doctrine and actions reflect the potential of cyber actions to degrade an adversary's decision-making capability. However, Russia emphasizes the information rather than the cyberspace aspect of its operations. It refers to "information space," which targets the cognitive domain rather than the artificial cyber domain (Giles 2016). Russian operations in the Georgian

conflict reflect Russia's attempt to shape the information campaign. Ambassador Mgaloblishvili (2017) stated that Georgian messaging was disadvantaged not because of loss of press websites, but because Russia had deployed 50 of its top journalists to Georgia in advance of hostilities.

Cyber warfare is most likely becoming an effective tool of already powerful states. Because cyber attacks are most effectively linked with more traditional kinetic forms of force, and due to the short nature of cyber advantage once capabilities are revealed, nations with capable militaries will be best equipped to exploit the type of advantage that cyber warfare gives. Strong powers are better equipped to threaten cyber attacks and to "reveal and replace" a given cyber capability to target an enemy's cyber vulnerabilities (Gartzke 2013). Although a host of cyber capabilities may be available to weaker actors, their effectiveness will be limited by their ability to exploit advantages generated in cyberspace. In cyberspace, the ability to alter regional or international balances or affect adversary's actions will be limited to those states that already possess considerable international influence.

References

Albright, D., Brannan, P., & Walrond, C. (2011). Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 report (ISIS Report). Institute for Science and International Security, Washington, DC. http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf. Accessed 22 Feb 2017.

Associated Press. (2008, March 11). Russia's NATO envoy says offering Georgia membership track would bolster separatists. *International Herald Tribune*. http://www.iht.com/articles/ap/2008/03/11/europe/EU-GEN-Russia-NATO.php. Accessed 11 Feb 2017.

Bennett, B. (2015, February 26). Cyberattacks pose growing threat to U.S., Intelligence Chief says. *Los Angeles Times*. Los Angeles. http://www.latimes.com/nation/la-na-intel-cyber-20150226-story.html. Accessed 3 Mar 2017.

Bonner, E. L. (2014). Cyber power in 21st-century joint warfare. *Joint Force Quarterly, 74*(3), 102–109.

Bowen, W. Q., & Brewer, J. (2011). Iran's nuclear challenge: Nine year and counting. *International Affairs (Royal Institute of International Affairs), 87*(4), 923–943.

Brenner, S. W. (2009). *Cyberthreats: The emerging fault lines of the nation state*. Oxford: Oxford University Press.

Bronk, C. (2016). *Cyber threat: The rise of information geopolitics in U.S. National Security*. Santa Barbara: Praeger.

Bumgarner, J. (2009). Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008. U.S. Cyber Consequences Unit. http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf. Accessed 11 Feb 2017.

Bumiller, E., & Shanker, T. (2012, October 11). Panetta Warns of Dire Threat of Cyberattack on U.S. *The New York Times*. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html. Accessed 16 Nov 2016.

Bussing, J. (2013). The degrees of force exercised in the cyber Battlespace. *Connections, 12*(4), 1–13.

Chivers, C. J., & Shanker, T. (2008, September 2). Georgia eager to rebuild its defeated armed forces. *The New York Times*. http://www.nytimes.com/2008/09/03/world/europe/03georgia.html. Accessed 22 Feb 2017.

Clarke, R. A., & Knake, R. (2011). *Cyber war: The next threat to National Security and what to do about it* (Reprint ed.). New York: Ecco.

von Clausewitz, C. (1989). *On War, Indexed Edition. (M. E. Howard & P. Paret, Trans.)* (Reprint ed.). Princeton: Princeton University Press.
Davis, J. (2007, August 21). Hackers take down the most wired country in Europe. https://www.wired.com/2007/08/ff-estonia/. Accessed 3 Mar 2017.
Department of Homeland Security. (2009). *National Infrastucture Protection Plan*. Department of Homeland Security: Washington, DC.
Echavarria, A., II. (2007). *Clausewitz and contemporary war*. Oxford: Oxford University Press.
European Parliament. (2008). European Parliament resolution of 5 June 2008 on the situation in Georgia. European Parliament. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2008-0253+0+DOC+XML+V0//EN&language=EN. Accessed 11 Feb 2017.
Farwell, J. P., & Rohozinski, R. (2012). The new reality of cyber war. *Survival, 54*(4), 107–120.
Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security, 38*(2), 41–73.
Giles, K. (2016). Handbook of russian information warfare (Fellowship monograph no. 9) (p. 90). NATO Defence College. http://www.ndc.nato.int/news/news.php?icode=995. Accessed 3 Mar 2017.
Hollis, D. (2011). Cyberwar case study: Georgia 2008. *Small Wars Journal*. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008. Accessed 11 Feb 2017.
Howard, M. (1989). The influence of Clausewitz. In P. Paret (Trans.), On war, indexed edition (Reprint edition, pp. 27–44). Princeton: Princeton University Press.
Johnson, D. E., Mueller, K., & Taft, W. H. (2003). *Conventional coercion across the Spectrum of operations: The utility of U.S. military forces in the emerging security environment*. Santa Monica: RAND Corporation.
Katznelson, I. (2013). *Baltic investment programme: Twenty years of joint Nordic financial and technical assistance to the three Baltic countries*. Copenhagen: Nordic Council of Ministers.
Kerr, P. K. (2016). Iran's nuclear program: Tehran's compliance with international obligations (No. R40094). Congressional Research Service, Washington, DC. https://fas.org/sgp/crs/nuke/R40094.pdf. Accessed 18 Feb 2017.
Korns, S. W., & Kastenberg, J. E. (2009). Georgia's cyber left hook. *Parameters, 38*(Winter 2008–09), 60–76.
Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal, Special Edition, 3*, 237–245.
Kushner, D. (2013). The real story of Stuxnet. *IEEE Spectrum, 50*(3), 48–53.
Libicki, M. C. (2014). Why cyber war will not and should not have its grand strategist. *Strategic Studies Quarterly, 8*(1), 23–39.
Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122.
Markoff, J. (2008, August 12). Before the Gunfire, Cyberattacks. *The New York Times*. http://www.nytimes.com/2008/08/13/technology/13cyber.html. Accessed 13 Feb 2017.
Mgaloblishvili, G. (2017, February 1). Phone interview.
Myers, S. L. (2007, April 27). Russia rebukes Estonia for moving Soviet statue. *The New York Times*. http://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html. Accessed 5 Mar 2017.
Nakashima, E., & Warrick, J. (2012, June 2). Stuxnet was work of U.S. and Israeli experts, officials say. *Washington Post*. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html. Accessed 6 Mar 2017.
Nuclear Threat Initiative. (2016). Iran: Nuclear. Nuclear Threat Initiative. Retrieved from http://www.nti.org/learn/countries/iran/nuclear/. Accessed 22 Feb 2017.
Nye, J. S. (2010). *Cyber Power*. Cambridge, MA: Belfer Center for Science and International Affairs.
Palmer, G., D'Orazio, V., Kenwick, M., & Lane, M. (2015). The MID4 data set: Procedures, coding rules, and description. *Conflict Management and Peace Science, 32*(2), 222–242.

Patel, T. (2011, April 21). Was INSAT-4B victim of malicious malware Stuxnet? *Indian Defence Review*. http://www.indiandefencereview.com/news/was-insat-4b-victim-of-malicious-malware-stuxnet/ . Accessed 1 Mar 2017.

Pukk, P. (2011). Goods in transit over the last decade. *Quarterly Bulletin of Statistics Estonia*, 104–112.

Richards, J. (2009). Denial-of-service: The Estonian cyberwar and its implications for U.-S. National Security. *International Affairs Review, 18*(2.) http://www.iar-gwu.org/node/65. Accessed 3 Feb 2017.

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939.

Russell, A. L. (2014). The Georgia-Russia war. In *Cyber Blockades* (pp. 96–127). Washington, DC: Georgetown University Press.

Sale, R. (2012, April 11). Stuxnet Loaded by Iran Double Agents. isssource.com. http://www.isssource.com/stuxnet-loaded-by-iran-double-agents/. Accessed 22 Feb 2017.

Sanger, D. E. (2012, June 1). Obama order sped up wave of cyberattacks against Iran. *The New York Times*. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. Accessed 21 Feb 2017.

Springer, P. J. (2015). *Cyber Warfare*. Santa Barbara: Springer.

Stone, J. (2013). Cyber war will take place! *Journal of Strategic Studies, 36*(1), 101–108. https://doi.org/10.1080/01402390.2012.730485.

Swaine, B. J. (2008, August 11). Georgia: Russia "conducting cyber war." *The Telegraph.* http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html. Accessed 14 Feb 2017.

Tagliavini, H. (2009a). Independent International Fact-Finding Mission on the Conflict in Georgia. Volume II. Council of the European Union. www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf. Accessed 11 Feb 2017.

Tagliavini, H. (2009b). The Independent International Fact-Finding Mission on the Conflict in Georgia. Volume I. Council of the European Union. http://www.mpil.de/files/pdf4/IIFFMCG_Volume_I1.pdf. Accessed 11 Feb 2017.

Tikk, E., Kaska, K., Rünnimeri, K., Kert, M., Talihärm, A.-M., & Vihul, L. (2008, November). Cyber attacks against Georgia: Legal lessons identified. Cooperative Cyber Defence Centre of Excellence. http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf. Accessed 12 Feb 2017.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford: Oxford University Press.

Wagstyl, S. (2007, May 3). Russia rail move to hit Estonian supply line. *Financial Times*. http://www.ft.com/cms/s/0/414f92b0-f928-11db-a940-000b5df10621.html?ft_site=falcon&desktop=true#axzz4aTcWvyMe. Accessed 5 Mar 2017.

Weinstein, D. (2014). Snowden and U.S. cyber power. *Georgetown Journal of International Affairs, International Engagement on Cyber, IV*, 4–11.

Williams, B. T. (2014). The joint force Commander's guide to cyberspace operations. *Joint Force Quarterly, 73*, 12–19.

Cyber Insurance

39

Pythagoras Petratos, Anders Sandberg, and Feng Zhou

Contents

P. Petratos (✉)
Said Business School, Oxford University, Oxford, UK
e-mail: Pythagoras.petratos@sbs.ox.ac.uk; p.pythagoras@yahoo.com

A. Sandberg
Oxford Martin Programme on the Impacts of Future Technology, Oxford University, Oxford, UK

Future of Humanity Institute, Oxford University, Oxford, UK
e-mail: anders.sandberg@philosophy.ox.ac.uk

F. Zhou
Future of Humanity Institute, Oxford University, Oxford, UK
e-mail: feng.zhou@philosophy.ox.ac.uk

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_25

Abstract

This chapter is an introduction to cyber insurance. We describe the different types or risks as well as uncertainty and ignorance related to cyber security. A framework for catastrophes on the cyber space is also presented. It is assessed which risks might be insurable or uninsurable. The evolution and challenges of cyber insurance are discussed and finally we propose some thoughts for the further development of cyber insurance markets.

Keywords

Catastrophic risks · Cyber insurance · Cyber risks/uncertainty/ignorance · Development of cyber insurance markets · Incentives · Insurable and uninsurable cyber risks

Introduction

Cyber insurance has a broad definition and has been continuously evolving over time. It was defined as insurance for the damages to "physical" computer equipment in 1970s, but nowadays it has been changed to be a cost-effective option of risk mitigation strategies for IT/cyber-related losses. According to Association of British Insurers (ABI), it "covers the losses relating to damage to, or loss of information from, IT systems and networks." Anderson et al. (2007) argue that cyber insurance in an ideal situation promotes users to implement good security. However, some barriers are currently preventing insurers to achieve this goal, and innovations in the cyberspace introduce new types of loss. For example, "Internet of Things" is shifting cybersecurity from protecting information assets to physical goods that were traditionally unrelated to computers.

At present, cyber insurance has a small share in overall nonlife insurance market and represents just 0.1% of the global property and casualty insurance premium pool (Marsh 2015), but it is one of the fastest-growing new lines of insurance business and the cybersecurity is recognized as one of the top global risks in the World Economic Forum's report recently (WEF 2015). Meanwhile, more and more traditional insurance contracts exclude specific losses that are linked to cybersecurity; it is necessary to develop a standalone cyber-insurance market. New technologies and innovations in the cyberspace are also spurring the development of cyber-insurance market, as well as the current trend of government requiring high standards on protecting sensitive information and enforcing financial punishments relating to information security breaches.

Both the complexity of cyber risk and the current immaturity of cyber-insurance market bring challenges for industry practitioners and regulators to fully understand potential future systemic risks in this kind of complex system. Not surprisingly, the recent Risk Nexus Report from Zurich Insurance Group argues that the global aggregations of cyber risk is analogous to those risks that were overlooked in the US sub-prime mortgage market (Zurich 2014). Its nickname "cyber sub-prime"

intends to describe the interconnected nature of systemic cyber risk and the challenges for individual insurers to address the complexity. They believe that the existing research on systemic risk in the financial markets that aims to address recent crises should be helpful to understand the dynamics of future cyberspace.

Development of Insurance for Cyber Risks

According to 2015 Information Security Breaches Survey (PWC 2015), 90% of UK large organizations and 74% of small businesses reported that they had suffered at least one security breach in the past 1 year. The average cost of the worst single breach suffered by these businesses has gone up sharply. For instance, the average cost to a large organization is around £1.5–£3 m up from £600 k to £1.15 m a year ago. The survey also indicates that the majority of UK businesses surveyed expect breaches will continue to increase. Thompson (2014) estimates that the total cyber insurance currently amounts around US$2 billion, whereas the total cost of global security breaches could be more than US$400 billion. For more about the effects of cyber-attacks on UK companies, see Oxford Economics (2014). For a more detailed history and evolution of cyber-insurance products, see Majuca et al. (2006).

Economics of Information Security

Together with both the growth of ICT (information and communication technology) and the growing impact of cyber risks to the real-world business increase the demand for insurance-related risk mitigation strategies. The following factors also play key roles in the development of cyber insurance:

A list of key factors affecting either demand for or supply of cyber insurance:

Mitigating cyber residual risks: Organizations have three basic cyber risk management strategies: self-protection, self-insurance, and transfer of risk via cyber insurance (Kesan et al. 2005). While organizations are increasing their information security spending on improving IT system, cyber residual risks still require insurance to mitigate unexpected events. Lelarge and Bolot (2009) find that cyber insurance is a powerful incentive mechanism that motivates organizations to invest in self-protection, so these three strategies are complementary to each other. Pal and Golubchik (2010) analyze the Internet users' investment in self-defense mechanisms when insurance solutions are offered in either full or partial cyber-insurance coverage models.

Promoting and aligning economic incentives: Organizations who have insurance as a last resort of risk management attract customers and business partners, especially for small businesses who are parts of a large/long supply chain in order to avoid being the weakest link of cyber-attacks. In the supply-demand model of cyber-insurance market, Pal (2014) argues that cyber insurance has the potential to jointly align the incentives of different stakeholders in the cyberspace, such stakeholders or players as security vendors, cyber insurers, regulatory agencies, and network users.

Anderson et al. (2007) also suggest that cyber insurance in an ideal situation promotes users to implement good security.

Protecting exclusions in traditional insurance: Cyber cover was mainly embedded in other traditional insurance products (e.g., business interruption or professional liability insurance), but nowadays more and more traditional insurance contracts intend to exclude the cyber-related risks due to the complexity of cyberspace and potentially catastrophic consequence, as well as requiring different actuarial methods to preform data analysis (Siegel et al. 2002). As a result, standalone cyber-insurance policies are emerged. However, there is a gap between insurers and insured parties to explain the differences/exclusions among both standalone cyber-insurance contracts and traditional products. It is necessary to have cyber-insurance brokers to reduce the gap (Marsh 2015).

Providing professional advice and delivering experienced cyber incident response: Insurance companies themselves collect a huge amount of customers' personally identifiable information and corporate clients' business confidential/financial information, so they must follow and have rich experience to deal with many regulations of protecting data information and cyber security (e.g., HIPAA Health Insurance Portability and Accountability Act to protect the privacy of individual patients/customers, GLBA Gramm Leach Bliley Act to secure the private information of clients) (Appari and Johnson 2010). Insurers also accumulate the updated knowledge and relevant experience from clients globally and communicate with other security professionals, in order to provide technical and legal assistance (as well as financial compensations) to manage cyber-related breaches and incidents (Marsh and Zurich 2015).

Training cybersecurity awareness and building information security culture: Security managers often find difficulties to communicate with nontechnical internal staff or external clients about security policies and technologies who have no formal security background, but insurance is an easy way to explain the (financial) impact of cybersecurity to the business. The insurance premium that has been reduced (or increased) year-by-year due to a better (or worse) security implementation in this year relative to other previous periods, it is a good indication and consistent comparison to define proper cyber risk metrics and to educate staff or clients. However, at this early stage of cyber insurance, there is still a lag for insurers to implement premium differentiation on the cyber insurance that reflects the insured security improvement precisely due to the immaturity of the cyber insurance market (Mukhopadhyay et al. 2013; Moran et al. 2015).

Government supports: A free-market approach is traditionally popular to manage risks in the financial system, since it increases motivation and efficiency of stakeholders in the system. As Anderson et al. (2007) suggest, one option to spur demand for cyber insurance is to make it compulsory (as it is common in motor insurance), but it may lead a deadweight on competitiveness and productivity growth. The role of government is to encourage and support the insurers to overcome the barriers of supplying cyber insurance (the barriers will be discussed in the cyber-insurance market section). Recently, UK government launched its "10 Steps to Cyber Security"

(CESG 2012) and "Cyber Essentials Scheme" (BIS 2014), both aiming to assist insurers to evaluate the security assessment of small- and medium-sized enterprises.

Sharing data of cyber incidents (data pooling): It is necessary to form partnerships from different industries that share data in order to better understand cyber risks, as suggested in the UK Cyber Security Strategy (Cabinet 2011). The recent launched Cyber Security Information Sharing Partnership (CiSP https://www.cert.gov.uk/cisp/) aims to collaborate with insurers to analyze emerging threats, disaster scenarios, and trends in the cyberspace. The cyber insurance will be more affordable and its purchasing cost is expected to be lower than current level based on more relevant actuarial data in the near future, and a higher degree of price differentiation across different policies and individual firms will be feasible (Marsh 2015). However, Bohme (2006) states and explains that information sharing is socially beneficial, but it is not efficient to rely on a trusted third party only (as a "social planner") to arrange data collection.

Insurable and Uninsurable Cyber Risks

In terms of a specific insurance policy, the potential losses related to cyber-attacks or nonmalicious IT failures can be currently grouped into 11 categories in the London Insurance Market (Marsh 2015), which is also similar to the US market (Majuca et al. 2006).

Due to both the difference in severity/frequency of cyber events and the complexity of cyber risks, some of these losses are insurable while others are not available at present. Johnson et al. (2014) study the complexity of estimating systematic risk in cyber networks, which is an essential requirement to provide cyber insurance to the public. The following discussion explains the insurability and exposure for different cyber risks (Marsh 2015).

Insurable Cyber Risks

Privacy events: Many privacy issues are related to managing regulatory requirements on information security. Insurers can collaborate with lawyers to provide different levels of services and protections to their clients. Since the losses from these events are handled and measured by a third-party professional lawyer, there is less information asymmetry or moral hazard problem between insurer and insured.

Crime and fraud: Police force often involves in the investigation of cyber-crime and fraud; therefore, the financial losses related to such cyber events are measured by third parties such as police or lawyers. Insurers can not only offer insurance cover, but also provide professional advice on preventing these events or reducing the cost based on their experience from other customers.

Network security liability: Third-party liabilities related to certain security events occurring within an organization's IT network can be insured, mainly due to the scope of incidents can be clearly defined by the insurers and IT system engineers can also collaborate with insurers to improve mitigation strategies.

Software and data damage: Insurers can provide indemnity for the costs arising from the damage of data or software (e.g., help recovering or reconstituting the damaged data); this is mainly because insurers are able to require the policy holders to follow necessary procedures of data backup or redundancy.

Cyber extortion: Traditionally, insurers have the necessary knowledge and experience of dealing with extortion in the physical world and conduct ransom negotiations (particularly in the London Market, such as the Lloyd's of London), extortion in the cyberspace is not much different from that. Cover is provided for both the cost of handling the incident and the ransom payment.

Uninsurable (or Insurable but with Constraints) Cyber Risks

Reputational loss: Although insurance cover is available for the losses that are directly linked to reputational damage (e.g., cost of recovering public image or loss revenue from existing customers), it is difficult to measure the value of the compensation and the linkage between the cyber incident and the intangible asset if without certain constraints.

Network business interruption (e.g., due to Denial-of-Service attacks): In the traditional insurance sector, it is common to offer full coverage for business interruption arising from natural disasters or man-made events. However, in the early stage of cyber insurance, insurers are concerned about the potential aggregate exposure from a single cyber event but interrupts many insured policy holders.

IP theft or espionage: These types of losses are extremely difficult to prove and quantify, since the value is changing quickly over time and trade secret is priceless before an incident but (likely) worthless if being public. It is also hard to define whether the incident was incurred in the insured period. Moreover, these attacks are often state-sponsored with a large amount of resource.

Physical asset damage: The interconnection between physical world and cyberspace is increased by the development of the so-called "Internet of Things (IoT)"; therefore, more and more cyber incidents will directly have impacts on the physical assets. At this stage, the complexity of these interconnections is not well understood by insurers; therefore, it is difficult to combine cyber insurance with traditional property insurance or have such physical asset damage cover in the standalone cyber insurance.

Death and bodily injury: Similar to the physical asset damage, it is more and more likely that certain cyber-related incidents may cause harm to the human (e.g., medical devices, large-scale industry equipment, driverless cars, etc.). Although it is uninsurable at the current stage of cyber insurance, it is covered by traditional insurance products such as general liability and employers' liability products (Fig. 1).

Challenges and Developments

Even if insurers are able to offer cyber insurance to mitigate certain types of cyber-risk events, they must face and learn to overcome some challenges in order to maintain and expand their businesses. Not surprisingly, there are progresses and developments to address these challenges recently.

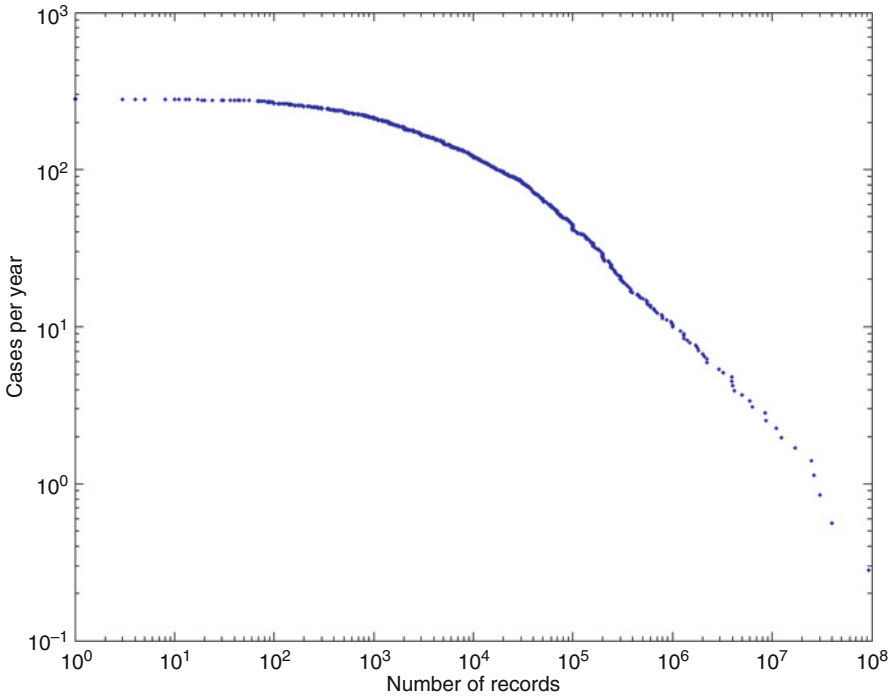


Fig. 1 Size distribution of data losses (based on data from datalossdb 2000–2005). Expected number of losses per year larger than a certain size as a function of number of records lost. Note the power-law heavy tail for larger losses (exponent ≈ -0.66, consistent with the results in Overill and Silomon (2011) and Maillart and Sornette (2010)). This tail may be dominated by more targeted events and organized crime, including financial fraud, insider abuse and theft, as well as malware (Overill and Silomon 2011).

Challenges for Insurers

External attackers are evolving over time: Information Security Breaches Survey (PWC 2015) shows that outsiders are using more sophisticated methods to affect organizations.

Staff-related breaches are unique in individual cases: Whether inadvertent human error or not, the consequence from insiders' mistakes or misconducts is difficult for insurers to measure.

Lack of understanding and communication: Recent surveys indicate that a majority of CEOs believe their organizations have relevant insurance to cover cyber risks (PWC 2015), whereas in fact only around 10% actually do (Marsh 2015).

Increasing IT system collaboration and social network: Cyberspace is moving toward an ecosystem, which has more and more heterogeneous players collaborate and interact to each other.

New technologies and innovations: The ICT sector is attractive to capital markets with large amounts of capital to support new businesses and innovations. However,

due to the nature of this fast evolving sector and heavy competition, ICT vendors focus more on the short process of introducing their products and services to the market and less on the security. It is challenging for insurers to follow these fast developments and potential risks involved in the process (Friedman 2011).

Recent Developments

Government: Organizations are increasingly using Government alerts (e.g., the UK HMG Cyber Essentials scheme) to inform their awareness of threats and similar vulnerabilities (PWC 2015). Insured firms can get discount on insurance premium if they follow these certification requirements, so it offers motivations for insured users to follow security procedures and policies.

Insurance cyber gap analysis: Marsh (2015) also suggests that it is necessary for insurance brokers to provide cyber gap analysis (determining which cyber risks are covered by existing traditional insurance or need to be covered in a standalone cyber insurance) when communicating with customers.

Insurers' data protection regulations: Insurance industry itself collects sensitive personal, financial, and healthcare data from their policy holders (e.g., personally identifiable information PII, protect health information PHI, and business operation private information) in order to measure the customers' risks more precisely. As a result, the National Association of Insurance Commissioners NAIC (2015) recently adopted cybersecurity guidance for the insurance industry and regulators to follow. The expertise and experience of insurers' information security practice is also applied to advice their customers.

Understanding the benefits of cyber insurance: The growing amount of literature starts to support the benefits of cyber insurance as a market-based solution to cybersecurity. Kesan et al. (2005) state, when certain obstacles to a full market solution are fully worked out, several positive outcomes will occur. In general, cyber insurance market will result in higher overall social welfare.

Evolution of Cyber-Insurance Market

It is still too early to know the structure of the future, mature cyber-insurance market. In the existing literature, both competitive (Shetty et al. 2010b) and monopolistic (Lelarge and Bolot 2009; Hofmann 2007; Pal and Golubchik 2011) market structures are studied.

As commonly expected, the cyber-insurance market will soon become a complex dynamic system (Anderson and Moore 2009; Halse and Hoemsnes 2013). As a result, the market not only provides one option of risk mitigation strategies, but also builds an ecosystem together with other sectors in cyberspace that can influence heterogeneous stakeholders' behaviors and business strategies (Hall et al. 2011). This is similar to other financial systems, such as stock or credit markets (Gracie 2015). Therefore, the existing research in other financial systems will be relevant to understand the future cyber-insurance market (Zurich 2014).

Obstacles of Developing Cyber-Insurance Market

Shetty et al. (2010a) and Bohme and Schwartz (2010) argue that the underdeveloped cyber insurance market is mainly due to: (1) interdependent security (externalities) (Ogut et al. 2005; Bolot and Lelarge, 2008; Zhao et al. 2009); (2) correlated risk (Bohme and Kataria, 2006); and (3) information asymmetries (Bandyopadhyay et al. 2009). Furthermore, Bohme and Schwartz (2010) argue that "it appears that the market failure can only be overcome if all obstacles are tackled simultaneously." Meanwhile, Marsh (2015) states that a well-developed reinsurance market for cyber insurance is also one of the necessary conditions to expand the business.

The four key obstacles are explained as follows:

Interdependent security (externalities): Kunreuther and Heal (2003) ask the question: "Do firms have adequate incentives to invest in protection against a risk whose magnitude depends on the actions of others?". One of the differences between cyber and traditional insurance (e.g., property or motor) is the close interconnections among players in cyberspace. The security in cyberspace is dependent on all players in the system, but heterogeneous players have different preferences about cybersecurity and the "free rider problem" occurs when those who benefit from other players' security investment do not have to pay for it (Varian 2004). As Naghizadeh and Liu (2014) argue that security is a nonexcludable public good, so users can stay out and still enjoy spill-overs from others' contribution without paying. As a result, even insurers help their insured customers to increase their overall security, those uninsured players in the system still can weaken these insured customers.

Correlated risk: Bohme and Kataria (2006) define two tiers of correlated cyber risks: (1) internal correlation, which they define as "the correlation of cyber risk within a firm" (i.e., a correlated failure of multiple systems on the internal network), and (2) global correlation, as "the correlation of cyber-risk at a global level, which also appears in the insurer's portfolio." The growing development of Cloud computing platform may accelerate the two tiers to be integrated together. For example, an internal incident in a cloud service provider will lead systematic risks in both its internal system and its customers' systems.

Information asymmetries: Bohme and Schwartz (2010) define "asymmetric information" as environment where some players have private information to take advantages on something that are not available to other players. The common issues in the conventional insurance literature due to "asymmetric information" are: adverse selection (Akerlof 1970) and moral hazard (Arrow 1963). They are also relevant to the cyber-insurance market and other obstacles (e.g., the interdependent security) may exacerbate its problems (Shetty et al. 2010a). Furthermore, Bohme and Schwartz (2010) also identify specific forms of information asymmetries in cyber insurance. Meanwhile, Pal (2012) proposes three mechanisms (premium differentiation, fines, security auditing) to resolve information asymmetry in cyber insurance.

Lack of reinsurance market: It is still in the early stage for reinsurers to reinsure cyber risks from primary insurers, but several proposals have been put forward to build such reinsurance function (Toregas and Zahn 2014), such as to establish

government-regulated funds similar to US Terrorism Risk Insurance Act or UK Financial Service Compensation Scheme. Anderson et al. (2007, 2009) discuss that one possible option is for government to provide reinsurance, but they emphasize that "while government re-insurance can create insurance markets where otherwise there would be no supply, such measures must be carefully designed to avoid a regime in which profits are private (to the insurers' shareholders), losses are socialized (born by the tax-payer), and systems remain insecure (because the government intervention removes the incentive to build properly secure products)."

Technologies Spur the Cyber-Insurance Market

Many new technologies that have been developed in recent years will spur the cyber-insurance market. We identify some of these technologies and group them into three main categories: (1) IT technologies assist insurers to manage and discover cyber incidents, as well as attract more customers demand for cyber insurance; (2) Technologies and methods that are helpful for insurers to perform actuarial modeling and data analysis; and (3) Technologies that are useful to better understand the complexity of cyber-insurance market.

IT Technologies

Some standalone technologies: Intrusion detection systems (IDS), firewalls, digital forensic technology, Microsoft Photo DNA, and encryption tools have become more advanced and relevant for insurers to investigate cyber incidents.

Trusted computing infrastructure: Although the opponents of trusted computing argue that users will lose their freedom and privacy (Anderson 2003a, b), the technology provides insurers an opportunity of identifying insurable events and defining claims more precisely.

Cloud platforms: Cloud service providers can reduce the issues of misaligned incentives between insurers and cloud users, if they can collaborate with insurers to attract more customers. Meanwhile, automated systems reduce human errors in the computing process. However, on the other hand, the cloud platform may lead to systemic risk since they are connected to other IT systems.

Anonymous communication and transactions: The anonymity network that is currently represented by, e.g., Tor software makes cyber criminals "anonymous" and untraceable. Anonymous digital currencies allow sophisticated markets for illicit goods and services (Juels et al. 2015). As a result, there is a deep/dark web that provides a cyber black market for attackers to trade sensitive information (e.g., selling stolen credit card information to other parties, etc.), so the attackers' motivation of attacking any organizations become larger.

Mobile devices: Nowadays, more and more business activities and collaborations are based on mobile devices (e.g., Bring Your Own Devices). This leads more cyber incidents that require cyber insurance, since such devices are lost or

stolen easily and users do not have sufficient skills to manage the security on these mobile devices.

Leaking technology: ICT enables rapid copying and dissemination of information, making information leaks harder to contain. In the past, a sizeable leak of proprietary information (such as more than 40 gigabytes of internal data released in the 2014 Sony hack) would have been limited by the need to transmit it by sending hard drives (expensive) or setting up a website (legally traceable and blockable); by 2014, it could be distributed anonymously using bittorrent in a way that makes it impossible to trace and block. In addition, leaks are potentiated by the appearance of search tools making released data more accessible.

Actuarial Modeling Methods

Network simulator: Similar to stress and scenario testing that are commonly used in the financial markets (e.g., banking system), insurers can use various applications and services to run network simulation in an artificial environment in order to test the stability and resilience of insured network under different conditions.

Actuarial data analysis (big data analytics): More and more professional consulting service firms have been investing and offering advanced actuarial pricing and risk management services based on big data analytics to assist insurers uncovering hidden patterns and unknown correlations in cyber risks.

Data pooling platform (data anonymization): Technologies of information sanitization that aim to encrypt or remove sensitive information from data sets are becoming more feasible; this encourages more data to be shared in the pooling platform in order to help government and insurers to better understand cyber risks from aggregated data sets.

Machine learning and Bayesian networks: More and more applications from these subfields of computer science are used in understanding the cyber risks. Insurers will hopefully gain insights about managing the cyber risks from these developments. Yang and Lui (2014) apply Bayesian network to analyze the influence of cyber-insurance market to security adoption in heterogeneous networks.

Data visualization: According to the "digital detectives" website of Microsoft, advances in data visualization technology assist Microsoft Digital Crimes Unit (uses Microsoft PowerMap) to understand the pattern of Citadel botnets better and remove the malware from infected machines more efficiently (Constantin 2013). The same technologies will help insurers to identify cyber incidents from different malware or causes, so they can distinguish the incidents in order to reduce specific claims (similar to distinguish different risk events in natural catastrophe insurance) or issue insurance-linked securities based on specified triggers (cyber incident) earlier. Anderson et al. (2007) consider one of potential strategies to promote cyber insurance is to develop financial instruments for risk sharing similar to "Cat Bonds" and "Exploit Derivatives" in the traditional insurance business operations (e.g., flood and natural-disaster insurance). As Anderson et al. (2007) explain, "Exploit Derivatives are vehicles for insurers to hedge against the discovery of vulnerabilities that causes significant loss events across their portfolios."

Sociotechnical Systems

Security awareness training and behavioral games: Toregas and Zahn (2014) mention a growing consensus that cyber security is not achievable by solely focusing on technological aspects, but also requiring to understand both technologies and their users' behaviors. The importance of understanding human-computer interaction has been studied widely since the works of Adams and Sasse (1999) and Sasse et al. (2001). Recently, some behavioral digital games based on computer simulations are introduced to train the users' behavior and awareness of using technologies securely (Cone et al. 2007).

Existing interdisciplinary research in financial systems: Bohme (2010b) argues that some key obstacles causing cyber-insurance market failure are due to a lack of understanding information economics. An interdisciplinary and integrated research that focuses on a cyber ecosystem is better than targeting each individual technological elements alone (Bohme, 2010a). This idea is similar to recent progress of understanding systemic risks in the financial markets. Schneier (2002) and Anderson and Moore (2007, 2009) state that a combination of economics, game theory, and psychology is necessary to understand and manage cybersecurity in the modern and future networked environment. Johnson et al. (2011) model security games with market insurance to inform policy makers on adjusting incentives to improve network security and cyber-insurance market. Baddeley (2011) applies some lessons from behavioral economics to understand issues of information security. More papers on the economics of information security and privacy can be found in the book of Moore et al. (2010).

Multiagent technique: Agent-based approach of modeling a complex system is becoming popular in the financial markets, but it is not commonly used by researchers to model cyberspace or perform stress testing on particular cyber events. Recently, a few researchers start to apply this technique to model network resilience (Sifalakis et al. 2010; Baxter and Sommerville 2011; Sommerville et al. 2012).

General Categorization of Cyber Risks

In the previous analysis, we presented the literature related to the evolution of cyber-insurance. It is our intention to further examine the challenges for the development of a cyber-insurance market. "An understanding of insurance must begin with the concept of risk – that is, the variation in possible outcomes of a situation" (Zeckhauser 2008). We embark on a theoretical and empirical analysis, using examples of cyber security events, in order to better understand cyber risks and relate them to cyber security.

The first crucial observation is that numerous different things can be included under the term "cyber risks." A more precise definition of "cyber risks" would result if we break them into three distinct elements.

- (Cyber) *Risk* can be defined as a measurable quantity, according to Knight (1921). In that sense, probability distributions could be assigned to cyber threats. Thus, it

is feasible to quantify the (cyber) risks and consequently estimate insurance premiums.

- (Cyber) *Uncertainty* can be considered to be the unmeasurable quantity related to cyber events. Therefore, we do not know the states of the world and the precise probabilities would not be known. It is also known as Knightian Uncertainty, based on the classic distinction by Frank Knight (1921).
- (Cyber) *Ignorance* can be considered a third category, when we may not have the ability to define what states of the world are possible (Zeckhauser and Visusi 2008). It can be considered one step further from uncertainty, when some potential outcomes are unknowable or unknown (Zeckhauser 2006). There are two important types of ignorance. *Primary ignorance* concerns situations in which one does not recognize that is ignorant and *recognized ignorance,* when one perceives that ignorance (Roy and Zeckhauser 2013). For example, the financial meltdown of 2008 can be considered such an event. It can also be argued that many catastrophic risks are subject to ignorance.

Catastrophic Risks and Insurance

General Description of Catastrophic Risks

The above general categorization brings us to further types of risk that influence cyber insurance. "Catastrophes provide the predominant conceptual model of what insurance is about. One pays premiums to secure financial protection against low-probability high consequence events – what we normally call catastrophes." (Zeckhauser 1996a, b). The main problem is that private markets are facing difficulties in providing coverage for catastrophic risk and thus they can be deemed "uninsurable risk" (Jaffee and Russell, 1997).

The timing and consequence of catastrophic events may largely vary. We have already identified the frequency/severity spectrum used for cyber events. In other words, the catastrophic risks fall within the low probability-high consequence class (Kleindorfer and Kunreuther 1999). However, the probabilities and consequences are not clearly defined, particularly toward the upper end of losses.

In this chapter, we are more interested about the insurers' perspective on assessing such risks. The Actuarial Standard Board defines "Catastrophe – A relative infrequent event of phenomenon that produces unusually large aggregate losses." More precisely, "An event is designated a catastrophe by the industry when claims are expected to reach a certain dollar threshold, currently set at $25 million, and more than a certain number of policyholders and insurance companies are affected"(Insurance Information Institute 2015). In that sense, numerous cyber events, as we would examine later, can have the rarity and loss magnitude of catastrophic risks.

However, catastrophes can involve a loss much greater than $25 million. The *Swiss Re Sigma Study* describes catastrophe losses. In 2014, total insured and uninsured losses due to disasters were estimated at $110 billion (Swiss Re 2015). This number is below the inflation adjusted 10 year average of $200 billion and

lower than $138 billion in 2013. However, the number of natural disaster catastrophes was at a record high reaching 189, and in total, there were 336 disaster events.

This variation in total losses and the number of catastrophes partly displays their unpredictability as well as their severe consequences. By doing simple calculations, we can observe that the average loss per catastrophe is much higher than $25 million (insurance covered claims of USD 28 billion of losses from natural catastrophes and USD 7 billion from man-made disasters). There are two major categories regarding the causes of catastrophic risks:

- Natural disasters, including georisks (like earthquakes) and climate-induced risks (as hurricanes and floods)
- Man-made catastrophes can be considered a broader category and it includes industrial accidents and terrorist attacks (Zurich 2013).

Earthquakes can have devastating effects for insurers but also situations are there where thousands of women claim to be damaged by breast implants or individuals harmed by asbestos (Zeckhauser 1996a, b). This example, except making the distinction between natural and man-made disasters, presents some interesting features that could be used for some initial comments about cyber risks.

A feature is that natural disasters are usually localized (geo specific). The same can apply to cyber events. A system failure in an energy grid can have local effects. Nevertheless there are many cases, let us say a computer virus,that can have regional or global impacts. Cyberspace is by its nature fairly nonlocal, and there are fewer "natural boundaries" that constrain the size of an impact. This makes these breaches rather easily diffuse around the world, therefore resulting in widespread damage.

Also, it seems that a disproportionately larger number man-made breaches and disasters occur in cyberspace (PWC 2015): actually it can be argued that there are very few cases in which the human factor is not involved. While the majority may be unintentional, intentional incidents have the potential for particularly expensive damage.

Aggregate Catastrophes and Systemic Risks

"Aggregate catastrophes occur when many similarly situated people, all subject to common risks, suddenly find that they have suffered a loss, and the total losses exceed expectations" (Zeckhauser 1996a, b). The *single worst* incident suffered by an organization might be considered to be a measure for informing us about catastrophic risks, especially in large corporations. Infection of viruses or malicious software remains the largest single worst incident causal factor (PWC 2015). As argued above, viruses and malware have the ability to propagate rapidly and cause harm to various people and organizations.

In that sense, we can further decompose the high consequence characteristic. One dimension is the number of individuals and organization that a cyber event might affect. Another dimension is the geographic location where the cyber event takes place. Some cyber events might have global reach, enlarging the consequences.

An additional critical parameter is the importance of the individuals and organization for the economy and society. A cyber-attack on critical infrastructure can further enlarge the consequence by generating losses to other operations. For example, the failure of VISA or MASTERCARD systems would not only result in losses for these companies, but it would likely generate significant losses to other businesses. This would apply to other critical (information) infrastructure, and the losses could be identified according to the importance of the system for the operations of other individuals and organizations.

Global Aggregations of Cyber Risk

A report by Zurich and the Atlantic Council attempts to expose "global aggregations of cyber risk" as analogous to the risks associated with the US sub-prime and 2008 financial crisis. "Governments and forward looking organizations need to take a holistic view and look beyond these issues to broader risks, including the increasing danger of global shocks initiated and amplified by the interconnected nature of the internet" (Zurich 2014). An illustrative analogy between the financial markets and the information technology of organizations is over-leverage (Zurich 2014). Over-leverage of companies in financial markets was created due to excessive debt, while organizations can over-leverage in IT due to overreliance on technology solutions. In both cases, leverage is used to maximize their returns; however, it is likely that the associated risks were underestimated, as it was proved by the financial crisis.

There are two crucial elements in this discussion. The first is a "Lehman moment," a catastrophic event that would spread in the web and cause major losses. Nevertheless a "Lehman moment" would encompass ignorance. While it was anticipated that Lehman Brothers could go bankrupt, none could foresee the chain of events that it triggered and led to the global financial crisis of 2008. In that sense, even catastrophic events that seem to have a specific impact might actually end in unpredictable outcomes. The original "Lehman moment" can be regarded a global shock due to the scale of Lehman Brothers operations across the world. However, the channel that initially cascaded this global shock was rather localized; the US sub-prime market.

The other element comprises of the propagation mechanism. The complexity and interconnections of financial products and markets eventually transmitted this shock around the globe. The complexity of financial products might be a useful analogy to the increasing complexity of IT systems. It has been argued that the 2008 financial crisis is a demonstration that the causes of risks were camouflaged by excess complexity (Zurich 2014). Even if this complexity is not excessive, it is still difficult to understand and predict the cascading risks and channels. Another analogy of the internet with the financial markets is that risks were assumed not to be correlated with each other. Nevertheless this is far from true: financial products and markets can be highly correlated. The same applies to information technology operations and systems.

In that sense, it is not only complexity per se but also complexity due to the interconnected nature of risks that add to the uncertainty (Zurich 2014). Thus, complexity and interconnections can facilitate systemic problems when "extreme

events," as global shocks, occur. "Connecting to the internet means exposure to nth-order effects – risks from interconnections with and dependencies on" other risk aggregations (Zurich 2014). The report by Zurich identifies seven such aggregations (internal IT enterprise, counterparties and partners, outsourced and contract, supply chain, disruptive technologies, upstream infrastructure, external shocks). It can be however argued that due to ignorance, they can be more common, or more severe, than expected (for example, external shocks). An addition issue is a possible "perfect storm." Especially if a cyber "Lehman moment" coincides with other events, this interaction could cause losses of much larger scope, duration, and intensity, similar to the series of events of the 2008 financial crisis (Zurich 2014). It is even more difficult or rather impossible to identify and define the interconnections between other events and a "Lehman moment" before it happens, since it is principally unpredictable. In the worst case, catastrophic events would coincide and can significantly multiply the damage. This makes mitigation of risks increasingly difficult, if the outcomes are unknown or unknowable.

Global Catastrophic Risks Framework

A very useful framework in order to qualitative describe globally catastrophic or existential catastrophes was developed by Nick Bostrom (Bostrom and Cirkovic 2011; Bostrom 2013). This framework is based on three factors: *severity* (how badly the population would be affected), *scope* (the size of the population at risk), and *probability* (how likely the disaster is likely to occur, according to the most reasonable judgment given currently available evidence). This model uses the first two factors and presents many advantages and flexibility. The scope includes not just the spatial size of the risk variable that we descried earlier, but also generational effects that are important regarding the duration and aftermath of the catastrophe.

Nevertheless, the major advantage of this framework is the way it treats probability. "Probability can be understood in different senses. . .The uncertainty and error-proneness. . .of risk is itself something we must factor into our all-things considered probability assignments. This factor often *dominates* in low-probability high-consequence risks – especially those involving poorly understood natural phenomena, complex social dynamics, or new technology, or are that difficult to assess for other reasons" (Bostrom 2013). Therefore, this facilitates our analysis since most of the factors discussed above can be adapted to this framework. Scope encompasses both geographic spread, number of affected actors, and the importance of the damage. Moreover, its flexibility allows adding other concepts. In the discussion that follows, because the uncertainty and ignorance surrounding the estimation of probabilities, we would shortly discuss about plausibility. Plausibility can be used as a distinct alternative to probabilities (Ramirez and Selin 2014) (Fig. 2).

Interdependencies and Asymmetric Threats

We have discussed correlations and interconnections. Special mention should be attributed to interdependencies, a related concept and relevant to cyber risks.

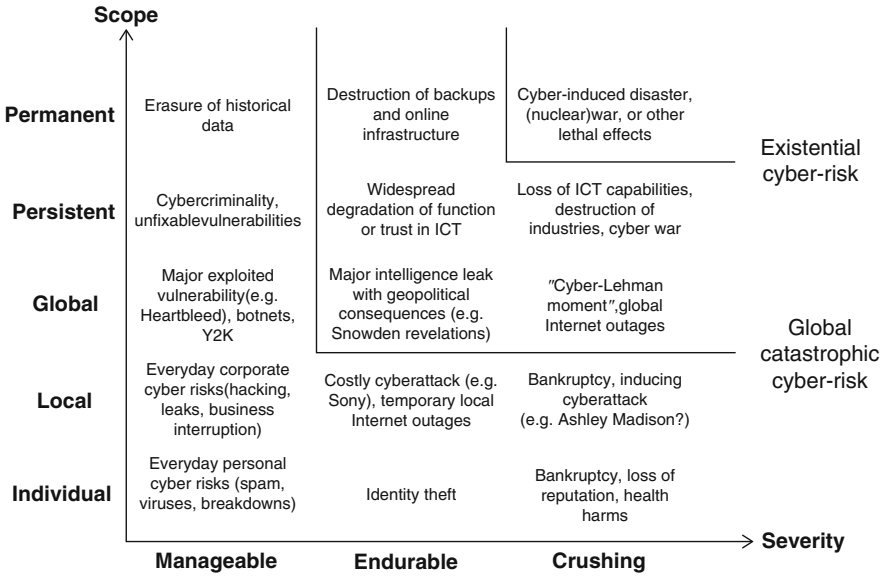


Fig. 2 Qualitative risk categories

Often these concepts are used interchangeably and denote the same thing. However, we would like to expand our analysis by focusing on complex interdependence (Keohane and Nye 1977, 1998), since it can provide an additional theoretical foundation. First of all, it should be emphasized that the context of international relations is central to insurance. Except political risk insurance, state relations influence numerous macrorisk factors, as economic relations and defense and security. "The information revolution alters patterns of complex interdependence by exponentially increasing the number of channels of communication in world politics" (Keohane and Nye 1998).

In addition, commercial and, particularly, strategic information are valuable. The availability and confidentiality of such information in multiple channels increases the level of risk. Information can be used to convince and capture terrorists, prevent and resolve conflicts, and enable countries to defeat adversaries (Nye and Owens 1996). On the other hand, because information reduces the "costs, economies of scale, and barriers of entry to markets, it should reduce the power of large states and enhance the power of small states and non-state actors" (Keohane and Nye 1998).

This generates important asymmetries. A small group of hackers could disrupt a relatively, to their size and resources, large IT system. Another notable case is that of WikiLeaks: a single leak, amplified by a single disseminating organization, has global consequences for a superpower. Asymmetric threats and the enabling of non-state actors add even more complexity to the layers described before. The number of threats is therefore multiplied and consequently risks increase. Moreover, ambiguity regarding the nature and identification of these relatively small actors makes the estimation of risks quite unpredictable.

Cyber Risks and Losses

Before 1989, the insurance industry did not experience a loss of more than $1 billion from a single event and since then catastrophes of the same magnitude have occurred (Kleindorfer and Kunrether 1999). As more and more people with larger insured wealth congregate in coastal areas, this is to expect (even leaving out climate change). "Megacatastrophes," like Hurricane Andrew, seem therefore to happen more often and clearly demonstrate the limitations of relying on historical data in order to estimate future probabilities of losses (Actuarial Standard Board 2000). Not only there are limitations to historical data, but also cyber risks are new phenomena with continuously evolving technology and factors that are difficult to predict or even imagine. However, it is argued that there is likelihood for a global cyber catastrophic event (Zurich 2014).

There are important methodological problems regarding probability estimation when assessing global catastrophic risks (Ord et al. 2010). Due to their high severity and scope, even low-probability risks need to be managed, but the probability of theory, model, or calculation error in doing so is far higher than the risk probability itself, even when done carefully. This means that risk estimates should be regarded as suspect unless bounded by several independent estimates or other constraints.

A major concern for the private insurance industry is that it might not be able to provide coverage for some catastrophic events without the possibility of insolvency or a significant loss (Kleindorfer and Kunreuther 1999). This is intensified when the scope and severity of the disaster are high. In the event of a "cyber sub-prime," the losses can be massive and potentially result to insolvency. Even more worried would be the possibility of interconnected events that could amplify such crisis. The coincidence of catastrophes or a perfect storm would also have devastating effects. It is therefore essential to try and understand the cyber risks that can affect insurance. In this part, we attempt to provide a theoretical analysis of risks in order to understand better cyber insurance. In the next part, we attempt to put some flesh to this theoretical skeleton by providing real and imaginary examples.

Cyber Risks, Catastrophes, and Ignorance

Identifying Cyber Risks

The discussion above indicated that the estimation of probabilities regarding cyber risks is in many cases difficult or impossible. The common methods are based on past events in order to define catastrophes and identify potential losses. These methods present significant limitations. There are various reasons for that. First of all, cyberspace is a very dynamic environment. Information and communication technologies are continuously changing. The internet is constantly expanding. It is embedding existing devices and technologies, and is likely to integrate future innovations, generating the Internet of Things (IoT). The number of interconnected devices, individuals, and organizations is therefore increasing. This results in larger

complexity and interdependence among devices with currently unknown functions and vulnerabilities.

In that sense, if we assume that we know all the causes of potential losses, then it might be a display of primary ignorance. On the contrary, we can recognize our ignorance. We attempt to examine practical examples of cyber risks in three ways. The first is though the traditional approach on historic events. The second technique can be considered an expansion of that. We can infer based on historical events and develop potential cases, subject to uncertainty. Finally, we would build imaginary but plausible scenarios (Ramirez and Selin 2014) in order to better understand cyber uncertainty and push the boundaries of ignorance. It can be said that effective scenario formation and imagining might reduce ambiguity, enter the space of ignorance, and therefore diminish it.

Existential and Global Catastrophic Risks

Bostrom's classification was developed in regard to threats to the entire future of the human species, or "merely" global disasters. The cyber counterpart would be risks that can escalate to such a level that they disrupt the global market or indeed current civilization. They are not merely uninsurably large, but terminal to most existing actors.

One possible example might be misuse of Artificial Intelligence (AI). Autonomous "smart" systems have already demonstrated potential for economically significant misbehavior such as the 2010 "Flash Crash," which at least in part was due to a systemic interaction of automatic trading agents. As technology advances, AI is likely to become more powerful and ubiquitous, but there are significant control problems that remain to be solved. The fundamental issue is that superintelligent systems do not generally behave in human-compatible ways, and this can produce existential risk (Bostrom 2013). More plausible scenarios involve unpredictable AI actions that are deliberate, autonomous, and potentially very tenacious. It might include the paralysis of the internet globally by AI software embedded in the web infrastructure, or by automated adaptive hacking tools (e.g., descendants of the current DARPA Cyber Grand Challenge). In another scenario of endurable severity and local scope, AI systems can involve the disruption of operations in an organization. Of course, severity may vary as well as scope. For example, if there is failure of ICT systems in a healthcare organization, it could result to loss of human lives. The disaster can diffuse globally if AI of a wide-spread logistics database system decides not to allow access to information, or even worse, altering or destroying it (for example, because it interprets restoration or circumvention attempts as intrusion attempts). However, due to the fact that the capabilities of AI are very ambiguous, such scenarios are difficult to define.

It may be that there are workable solutions or that AI will never be too powerful, but these are risky bets. It seems that it is easy for people to overestimate their knowledge regarding AI (Yudkowsky 2011). "It may be tempting to ignore Artificial Intelligence because, of all the global risk. . .AI is hardest to discuss. We cannot consult actuarial statistics to assign small annual probabilities of catastrophe, as with

asteroid strikes. We cannot use calculations from a precise, precisely confirmed model to rule out events or place infinitesimal upper bounds on their probability, as with proposed physics disasters. But this makes AI catastrophes more worrisome, not less." (Yudkowsky 2011). In that sense, AI qualifies for uncertainty and ignorance. AI represents a risk that could go all the way into the extreme upper right hand box of the framework, but is both extremely uncertain and largely a future risk: it can be dealt with by R&D aimed at safe and beneficial uses of AI.

However, cyber risk also has strong interconnections to traditional catastrophic risks. Such risks include major technical disasters, conflict and war, and particularly total war with the use of weapons of mass destruction (WMD).

The threat of a nuclear disaster is the most notable case by far. This is due to Stuxnet, a complex piece of malware interfering with Siemens industrial control systems and speculated that it was used for Iran nuclear program (NATO 2013). Based on this precedent, it can be argued that a nuclear catastrophe can be realized. The scale of these risks could largely vary. Cirincione (2011) and Ackerman and Potter (2011) discuss the global catastrophic risks of nuclear war and catastrophic nuclear terrorism. In both cases, cyberspace is "enabling" these risks. In addition, the internet could provide the most cost-effective opportunity for adversaries. It enables states and non-state actors and enhances their power. They can transform their capabilities and become nuclear threats that were not imaginable in the past. These asymmetric threats impose great challenges to insurance.

Stuxnet is considered to be a government cyber weapon. Rogue states might dedicate more resources in attaining such capabilities. The same could apply with terrorist groups. It is interesting to notice the multiple channels and complexity surrounding them. States relations can deteriorate and governments might decide to pursue cyber weapons targeting at nuclear as well as other military and critical infrastructure targets. The emergence of terrorist groups is also subject to uncertainty and ignorance. The rapid emergence of Islamic State, raising considerable resources, was not forecasted. Hamas and Hezbollah were established terrorist organizations and it can be alleged that they were capable of using cyber space. Nevertheless, it was believed by Israeli officials that these organizations used a criminal organization based in a former Soviet State to attack Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip (NATO 2013).

Cyber weapons can also easily be spread to other actors, through theft or leakage (such as the exploits revealed in the attack on the security consultancy Hacking Team in 2015), trade, or by imitation: once Stuxnet was out in the wild, many other groups could analyze it and copy its tricks into their toolkits. The market for zero-day exploits, driven by governments and security companies seeking new tools, has both the effect of incentivizing search for more vulnerabilities and inhibiting public disclosure of them since discoverers can gain more by secretly selling their find and agencies using them do not wish to lose their advantage. Even when vulnerabilities are revealed, removing them is sometimes hard since they might be embedded in systems that cannot easily be upgraded (such as industrial systems or implants); this means that use of some cyber weapons can lead to more subsequent attacks on targets unrelated to the original target.

This case highlights the complexity generated by multiple channels and agents. It is consistent with the concept of nth order effects (Zurich 2014). The potential cooperation of different agents enhances complexity due to the exponential number of combinations. Nexuses of adversaries can be formed, pooling resources and capabilities and thus magnifying cyber attacks. Nuclear catastrophes can have regional or global consequences (Cirincione 2011) according to their intensity. Similar cyber global catastrophic scenarios can involve other types of WMD (i.e., biological weapons) or conflict and war.

Catastrophic Risks

War and conflict enabled by cyber space can present variations in consequences and scale. They can also be interdependent to other complex events. The cyber-attack on Estonia in April 2007 was caused due to political frictions with Russia. On August 2008, the conflict of Russia and Georgia was accompanied by hacking activity from unknown foreign intruders which appeared to coincide with Russian military actions (NATO 2013). A crucial observation is that the manmade causes of these cyber attacks are still not known with certainty. Another critical remark is that there are interdependencies between traditional kinetic power and cyber capabilities. An analogous example to the above cases is the takeover of missile systems by hackers (there are claims this briefly happened to a German Patriot antiaircraft defense system in 2015 (Storm 2015)). An action by hackers launching missiles could escalate to conflict or war.

Now imagine that these missiles are stationed in South Korea. And that they are launched by unknown hackers just after the cyber-attack on Sony, that FBI blamed on Pyongyang (BBC 2015). Sony was about to release the interview, a comedy about the assassination of the North Korea's Leader, indicating that the tensions in North Korea were running high. This could trigger events that could escalate to a catastrophe involving even nuclear weapons. A crisis in Korea could also cause negative impact on global markets due to the importance of the South Korean economy and trade interconnections. This example presents just a small part of complex interdependencies.

This example could have been even worse. Imagine now that the aforementioned events coincide with a release on WikiLeaks that North Korea is abandoned and isolated (a previous WikiLeaks cable suggested that Chinese officials expressed the desire to relinquish support for North Korea (The Economist 2010)). North Korea can increase its level of alertness and retaliate severely, if they feel that the balance of power has changed against them and the regime is under existential threat. If these events coincide, then it is more likely to have a catastrophe. It is also possible that these events are fabricated and lead to an "accident." It is important to realize the multiple layers of complex interdependencies, which in many occasions can be unpredictable. The "WikiLeaks paradigm" is noteworthy because it can generate the conditions and instability which can consequently trigger other disasters.

In January 2011, the Canadian government reported an attack against its Department of National Defense as well as the Finance Department and Treasury Board,

causing the disconnection of the main Canadian economic agencies from the internet (NATO 2013). Once again, there is ambiguity regarding the identity of attackers, and in addition Canadian counter-espionage agents were left scrambling to find how much sensitive information was compromised (Weston on CBC News 2011). In that sense, it is not only difficult to forecast cyber-attacks but it is also unclear how much loss they caused. This makes mitigation harder. A proof of that is that cyber-attacks disrupted again the Department of Finance and Treasury Board (MacDonald and King on WSJ 2015). Thus, cyber-attacks are repeated with frequency on the same critical infrastructure.

Although these cyber-attacks might not qualify for catastrophic risks, it is hard to estimate the losses and associated costs. A considerable loss is the opportunity cost for not using the economic infrastructure of the Department of Finance and Treasury Board. Except Stuxnet, earlier, in 2003, Slammer worm disabled safety monitors in nuclear facilities and later, in October 2011, the Duqu Trojan hit Iran's nuclear facilities (Vaidya 2015). This is another indication of the frequency of cyber-attacks on nuclear facilities, which could easily lead to major catastrophes.

Not only nuclear facilities are targeted but also energy infrastructure has experienced cyber-attacks. A notable case is Shamoon malware which destroyed 30,000 computers of Saudi Aramco in August of 2012. Interestingly enough, 5 days later, a similar attack forced RasGas, one of the largest producers of liquid petroleum gas, to shut down its website and e-mails (BBC 2012). Despite that it was not reported oil and gas supply was not disrupted, inference to these cases points that in the future this is a plausible consequence. Especially similar cyber-attacks can create shocks to the global economy due to interconnections, if they coincide with other events affecting the price of energy.

We have mainly focused on cyber events that produce high consequence outcomes on a single or small number of organizations affected. Nevertheless, another important category of cyber events is when they have impact on a wide range of individuals and organizations. This type of events is likely to generate systemic global catastrophes. There are numerous examples. In respect to losses, some cases are distinct. Code Red Worm as early as July 2001 infected 359,000 computers in less than 14 h and caused estimated losses of $2.6 billion, Mydoom in 2004 skyrocketed losses to $38.5 billion, Conficker in 2008 infected 11 million hosts with an estimated loss of $9.1 billion, and the list is long (Vaidya 2015). It should be noted that these disasters are systemic and with correlated global effects. They can therefore be considered potential "Lehman moments" for cyber insurance.

Conclusion: Summary, Challenges, and Future Directions, the Development of the Cyber Insurance Market

Cyber risks are rapidly evolving due to technological change and the systemic and complex nature of the ICT world, producing fundamental uncertainty and ignorance. Cyber insurance typically focuses on the less uncertain risks or constrains uninsurable risks to make them more manageable. Tools or practices for handling

interdependent security, correlation, and information asymmetries as well as the lack of reinsurance would help the market grow.

While there are some cyber risks for which we can have sufficient information for quantifiable estimates, in the majority of cases, uncertainty and ignorance prevail. This reflects the very limited, if any, information regarding the nature and evolution of cyber-attacks. There are two basic problems in obtaining information. The first concerns the identity of attackers. The agents responsible for cyber threats present a large variety. They can range from large nations and militaries to organized crime and activists. The second issue, somewhat related to the first, are the resources and skills of these agents. The skills and sophistication can also substantially vary.

There are examples of single hackers that managed to cause catastrophic damage – like Michael Calce aka "MafiaBoy" – who has caused an estimated $1.2 billion damage with attacks on CNN, Dell, e-Bay, and Amazon (Niccolai 2000; Harris 2006). Organized crime groups (OCGs) are getting more involved in cyber crime, and trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims, and economic damage (Europol 2014). Nevertheless, except traditional OCGs that leverage their existing criminal activity, there are many new organized criminals focusing solely on cyber crime. They are capable of building sophisticated and complex systems for stealing money and intellectual property at a "grand scale," and it has been reported that in former Soviet Union there are 20–30 criminal groups that have reached "nation-state level" capabilities (Ranger 2014).

It has been argued that many governments are developing their cyber offensive and defensive capabilities, and most particularly cyber intelligence operations. US is further "aggressively" enhancing its cyber capabilities. This is because of claims by officials about serious cyber threats from China and occurrence of high-magnitude attacks, for example, on Sony from North Korea (Mason and Hosenball 2015). There is considerable uncertainty and ignorance regarding the nature and source of many threats. Often the perpetrating agents cannot be identified. On top of that, there are allegations that some governments might employ hackers or even organized cyber criminals. In this dynamic environment, threat agents can easily change identity and diffuse their knowledge and innovative technologies. At the same time, much information regarding these threats or attacks might remain unknown. Finally, cyberterrorist acts have been anticipated, but none can predict their potential scale. An analogy with the unexpected rise of Islamic State (IS) might be drawn.

In general, it is very hard or in some cases seems impossible to have information and predict the frequency and magnitude of cyber-attacks. At the same time, it is also difficult to estimate the potential losses from cyber-attacks due to interdependencies that can propagate shocks and strongly correlated risks. These, along with limited information regarding the reputation loss, opportunity cost from operation interruptions, valuation of intellectual property, among others, impose significant barriers to the development of insurance markets. In that sense, uninsurable risks can remain. Nevertheless, building better insurance and financial models, as some actuarial models referred above, is a first step to better understand and estimate cyber risks and relate them to insurance premiums. On top of that, incentives, regulation and

liability provisions, new technologies for better security, and investment in secure infrastructure can diminish some risks and facilitate the further development of cyber insurance markets.

It may be that these barriers are insurmountable, or that currently undiscovered tools – whether technological, actuarial, or social – are ready to be found. The challenge is extremely hard, involving management of systemic risks with elements of extreme uncertainty and ignorance, but the market rewards would be equally grand.

Acknowledgement This work was supported by the FHI-Amlin Research Collaboration on Systemic Risk of Modelling in pursuing better understanding and management of the systemic risks associated with modeling in the insurance industry through the strategic collaboration between the Future of Humanity Institute and Amlin. We are grateful for comments and suggestions from numerous colleagues and insurance industry participants from Amlin plc, the Lloyd's of London, and the Bank of England in several meetings and discussions among working parties.

References

Ackerman, G., & Potter, W. (2011). Catastrophic nuclear terrorism. A preventable peril. In N. Bostrom & M. Cirkovic (Eds.), *Global catastrophic risks*. New York: Oxford University Press.

Actuarial Standard Board. (2000). Treatment of catastrophe losses in property/casualty insurance ratemaking actuarial standard of practice no. 39.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40–46.

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *The quarterly journal of economics, 84*(3), 488–500.

Anderson, R. (2003a). Cryptography and competition policy issues with trusted computing. In Proceedings of PODC'03, Boston, MA, pp. 3–10.

Anderson, R. (2003b). 'Trusted computing' and competition policy – Issues for computing professionals. Upgrade. *The European Journal for the Informatics Professional, 4*(3), 35–41.

Anderson, R., Bhme, R., Clayton, R., & Moor, T. (2009). Security economics and european policy. In N. Pohlmann, H. Reimer, & W. Schneider (Eds.), *ISSE 2008 securing electronic Business processes* (pp. 57–76). Wiesbaden: Vieweg+Teubner.

Anderson, R., Bohme, R., Clayton, R., & Moore, T. (2007). *Security economics and the internal market*. Heraklion: ENISA.

Anderson, R., & Moore, T. (2007). Information security economics and beyond. Advances in Cryptology – CRYPTO07.

Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, 367*(1898), 2717–2727.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International journal of Internet and enterprise management, 6*(4), 279–314.

Arrow, K. J. (1963). Uncertainty and the welfare economics of medical care. *The American economic review, 53*(5), 941–973.

Baddeley, M. (2011). Information security: Lessons from behavioural economics. In Workshop on the Economics of Information Security.

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why it managers don't go for cyber-insurance products. *Communications of the ACM, 52*(11), 68–73.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 23*(1), 4–17.
BBC. (2015, January 3). Sony cyber-attack: North Korea faces new US sanctions. http://www.bbc.co.uk/news/world-us-canada-30661973.
BBC. (2012, August 31). Computer virus hits second energy firm. http://www.bbc.co.uk/news/technology-19434920.
BIS. (2014). Cyber essentials scheme. Technical report, UK Department for Business Innovation and Skills.
Bohme, R. (2006). A comparison of market approaches to software vulnerability disclosure. In *Emerging trends in information and communication security* (pp. 298–311). Berlin: Springer.
Bohme, R. (2010a). Security metrics and security investment models. In *Advances in information and computer security* (pp. 10–24). Berlin: Springer.
Bohme, R. (2010b). Towards insurable network architectures. *Information Technology, 52*(5), 290–293.
Bohme, R., & Kataria, G. (2006). Models and measures for correlation in cyber-insurance. In Workshop on the Economics of Information Security (WEIS).
Bohme, R., & Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. In Workshop on the Economics of Information Security (WEIS).
Bolot, J.-C., & Lelarge, M. (2008). A new perspective on internet security using insurance. In INFOCOM 2008. The 27th Conference on Computer Communications, IEEE.
Bostrom, N. (2013). Existential risk prevention as global priority. *Global Policy, 4*, 15–31.
Bostrom, N., & Cirkovic, M. (Eds.). (2011). *Global catastrophic risks*. New York: Oxford University Press.
Cabinet. (2011). The UK cyber security strategy: Protecting and promoting the UK in a digital world. Technical report, UK Cabinet Office.
CESG. (2012). 10 steps to cyber security: Information risk management regime. Technical report, UK Department for Business Innovation and Skills.
Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security, 26*(1), 63–72.
Cirincione, J. (2011). The continuing threat of nuclear war. In N. Bostrom & M. Cirkovic (Eds.), *Global catastrophic risks*. New York: Oxford University Press.
Constantin, L. (2013). FBI and Microsoft takedown program blunts most citadel botnets. Computer World.
Crowley J. (2011). 10 most costly cyber attacks in history. BusinessPundit.com. http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history/.
Europol. (2014). The Internet Organised Crime Treat Assessment (iOCTA) 2014. European Police Office.
Friedman, A. (2011). Economic and policy frameworks for cybersecurity risks. Center for Technology Innovation at Brookings.
Gracie, A. (2015). Cyber resilience: A financial stability perspective. Cyber Defence and Network Security Conference, London.
Hall, C., Clayton, R., Anderson, R., & Ouzounis, E. (2011). Inter-x: Resilience of the internet interconnection ecosystem. ENISA.
Halse, H. R. and Hoemsnes, J. (2013). Cyber-insurance and endogenous network formation. Master's thesis. Norwegian Unievrsity of Science and Technology.
Harris, J. K. (2006). Ethical perspectives in information security education. *Issues in Information Systems VII, 1*, 181.
Hofmann, A. (2007). Internalizing externalities of loss prevention through insurance monopoly: An analysis of interdependent risks. *The Geneva Risk and Insurance Review, 32*(1), 91–111.
Insurance Information Institute. (2015). Catastrophes and insurance issues. http://www.iii.org/publications/insurance-handbook/insurance-and-disasters/catastrophes-and-insurance-issues.
Jaffee, D. M., & Russell, T. (1997). Catastrophe insurance, capital markets, and uninsurable risks. *The Journal of Risk and Insurance, 64*(2), 205–230. Symposium on Financial Risk Management in Insurance Firms (June, 1997).

Johnson, B., Böhme, R., & Grossklags, J. (2011). Security games with market insurance. In *Decision and game theory for security* (pp. 117–130). Berlin: Springer.
Johnson, B., Laszka, A., & Grossklags, J. (2014). The complexity of estimating systematic risk in networks. In 27th Computer Security Foundations Symposium (CSF), IEEE, pp. 325–336.
Juels, A., Kosba, A., & Shi, E. (2015). The ring of gyges: Using smart contracts for crime. *Aries, 40*, 54.
Keohane, R., & Nye, J. (1977). *Power and interdependence: World politics in transition*. Boston: Little, Brown.
Keohane, R., & Nye, J. (1998). Power and interdependence in the information age. *Foreign Affairs, 77*(5), 81–94.
Kesan, J., Majuca, R., & Yurcik, W. (2005). Cyberinsurance as a market-based solution to the problem of cybersecurity: A case study. In Workshop on the Economics of Information Security (WEIS).
Kleindorfer, P., & Kunreuther, H. (1999). Challenges facing the insurance industry in managing catastrophic risk. In K. A. Froot (Ed.), *The financing of catastrophe risk*. Chicago: University of Chicago Press.
Knight, F. (1921). *Risk, uncertainty, and profit*. Boston, MA: Houghton Mifflin Co.
Kunreuther, H., & Heal, G. (2003). Interdependent security. *Journal of Risk and Uncertainty, 26*(2–3), 231–249.
Lelarge, M., & Bolot, J. (2009). Economic incentives to increase security in the internet: The case for insurance. In INFOCOM 2009, IEEE, pp. 1494–1502.
MacDonald A., & King C. (2015, June 17). Canadian government servers hit by Cyberattack, minister says hacking group anonymous takes credit for the attack, which appeared to have affected several government websites. *Wall Street Journal*. http://www.wsj.com/articles/canadian-government-servers-hit-by-cyberattack-minister-says-1434565899.
Maillart, T., & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. *The European Physical Journal B, 75*(3), 357–364.
Majuca, R. P., Yurcik, W., & Kesan, J. P. (2006). The evolution of cyberinsurance. arXiv preprint cs/0601020.
Marsh. (2015). UK cyber security: The role of insurance in managing and mitigating the risk. Technical report, UK HM Government.
Marsh, & Zurich. (2015). UK 2015 cyber risk survey report. Technical report, Marsh Insights.
Mason, J., & Hosenball, M. (2015, June 8) Obama vows to boost U.S. cyber defenses amid signs of China hacking. *Reuters*.
Moore, T., Pym, D., & Ioannidis, C. (Eds.). (2010). *Economics of information security and privacy*. New York: Springer.
Moran, J., Beeson, B., Mulligan, C., Sage, O., & Menapace, M. (2015). Examining the evolving cyber insurance marketplace. Homeland security digital library.
Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure it or not? *Decision Support Systems, 56*, 11–26.
Naghizadeh, P., & Liu, M. (2014). Voluntary participation in cyber-insurance markets. In Workshop on the Economics of Information Security (WEIS).
NAIC. (2015). Principles for effective cybersecurity: Insurance regulatory guidance. National Association of Insurance Commissioners.
NATO. (2013). The history of cyber attacks – A timeline. http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm.
Niccolai, J. (2000, February 10). Analyst puts hacker damage at $1.2 billion and rising, *InfoWorld*. Archived from the original on 12 November 2007. Retrieved 22 March 2007.
Nye, J., & Owens, W. (1996). America's information edge. *Foreign Affairs, 75*(2), 20–36.
Ogut, H., Menon, N., & Raghunathan, S. (2005). Cyber insurance and it security investment: Impact of interdependence risk. In Workshop on the Economics of Information Security (WEIS).

Ord, T., Hillerbrand, R., & Sandberg, A. (2010). Probing the improbable: Methodological challenges for risks with low probabilities and high stakes. *Journal of Risk Research, 13*(2). Special Issue: The Philosophy of Risk.
Overill, R. E., & Silomon, J. A. (2011). Single and double power Laws for cyber-crimes. *Journal of Information Warfare, 10*(3), 29–36.
Oxford Economics. (2014). Cyber-attacks: Effects on UK companies. Technical report, Oxford Economics (A report for Centre for the Protection of National Infrastructure).
Pal, R. (2012). Cyber-insurance for cyber-security: A solution to the information asymmetry problem. In SIAM Annual Meeting. Citeseer.
Pal, R. (2014). Improving network security through cyber-insurance. PhD thesis, University of Southern California.
Pal, R., & Golubchik, L. (2010). Analyzing self-defense investments in internet security under cyber-insurance coverage. In IEEE 30th International Conference on Distributed Computing Systems (ICDCS), pp. 339–347.
Pal, R. and Golubchik, L. (2011). Pricing and investments in internet security: A cyber-insurance perspective. CoRR, abs/1103.1552.
PWC. (2015). 2015 Information security breaches survey. Technical report, UK HM Government.
Ramirez, R., & Selin, C. (2014). Plausibility and probability in scenario planning. *Foresight, 16*(1), 54–74.
Ranger, S. (2014, June 9). Organised cybercrime groups are now as powerful as nations. *ZDNet*.
Roy D., & Zeckhauser R. (2013). Ignorance: Lessons from the Laboratory of Literature. M-RCBG Faculty working paper series 2010-11.
Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the weakest linka human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122–131.
Schneier, B. (2002). Computer security: Its the economics, stupid. In Workshop on the Economics of Information Security (WEIS).
Shetty, N., Schwartz, G., Felegyhazi, M., & Walrand, J. (2010a). Competitive cyber-insurance and internet security. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of information security and privacy* (pp. 229–247). New York: Springer.
Shetty, N., Schwartz, G., & Walrand, J. (2010b). Can competitive insurers improve network security? In A. Acquisti, S. Smith, & A.-R. Sadeghi (Eds.), *Trust and trustworthy computing*, *Lecture notes in computer science* (Vol. 6101, pp. 308–322). Berlin: Springer.
Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-risk management: Technical and insurance controls for enterprise-level security. *Information Systems Security, 11*(4), 33–49.
Sifalakis, M., Fry, M., & Hutchison, D. (2010). Event detection and correlation for network environments. *IEEE Journal on Selected Areas in Communications, 28*(1), 60–69.
Sommerville, I., Cliff, D., Calinescu, R., Keen, J., Kelly, T., Kwiatkowska, M., Mcdermid, J., & Paige, R. (2012). Large-scale complex it systems. *Communications of the ACM, 55*(7), 71–77.
Storm, D. (2015, July 8). Did hackers remotely execute "unexplained" commands on German patriot missile battery? *Computerworld*.
Swiss Re. (2015). Underinsurance of property risks: Closing the gap. Swiss Re.
The Economist. (2010, November 30). WikiLeaks embarrasses North Korea: A glimpse into the dark. *The Economist*. http://www.economist.com/blogs/banyan/2010/11/wikileaks_embarrasses_north_korea.
Thompson, M. (2014). Why cyber-insurance is the next big thing. In CNBC Report.
Toregas, C., & Zahn, N. (2014). Insurance for cyber attacks the issue of setting premiums in context. Cyber Security Policy and Research Institute, The George Washington University.
Vaidya T. (2015). 2001-2013: Survey and analysis of major cyberattacks. Working Paper. http://arxiv.org/pdf/1507.06673.pdf.
Varian, H. R. (2004). System reliability and free riding. In *Economics of information security* (pp. 1–15). Dordrecht: Kluwer Academic Publishers.
WEF. (2015). Global risks 2015. Technical report. World Economic Forum, Geneva.

Weston G. (2011, February 16). Foreign hackers attack Canadian government: Computer systems at 3 key departments penetrated. *CBC News*. http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618.

Yang, Z., & Lui, J. C. (2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation, 74*, 1–17.

Yudkowsky, E. (2011). Artificial intelligence as a positive and negative factor in global risk. In N. Bostrom & M. Cirkovic (Eds.), *Global catastrophic risks*. Oxford: Oxford University Press.

Zeckhauser, R., & Visusi, K. (2008). Discounting dilemmas: Editors' introduction. *Journal of Risk and Uncertainty, 37*(2), 95–106.

Zeckhauser R. (2008). Insurance. The Concise Encyclopaedia of Economics. http://www.econlib.org/library/Enc/Insurance.html.

Zeckhauser, R. (2006). Investing in the unknown and unknowable, capitalism and society. *Berkeley Electronic Press, 1*(2.) http://www.bepress.com/cas/vol1/iss2/art5.

Zeckhauser, R. (1996a). The economics of catastrophes. *Journal of Risk and Uncertainty, 12*(2), 113–140.

Zeckhauser, R. (1996b). Insurance and catastrophes. *Geneva Papers on Risk and Insurance: Issues and Practice, 78*, 3–21.

Zhao, X., Xue, L., & Whinston, A. B. (2009). Managing interdependent information security risks: A study of cyber-insurance, managed security service and risk pooling. ICIS 2009 Proceedings, p. 49.

Zurich. (2014). Beyond data breaches: Global interconnections of cyber risk. Risk Nexus Report of Zurich Insurance Group and Atlantic Council.

Zurich Insurance Group. (2013). Modeling natural catastrophes. Annual report 2013. http://www.zurich.com/2013/en/annual-report/risk-review/analysis-by-risk-type/insurance-risk/modeling-natural-catastrophes.html.

Cyber Documentation and Research Center "Horizon Scanning Center" for Cyber Analysis and Monitoring

40

Klaus Mak, Johannes Göllner, Peter Prah, Christian Meurers, and Joachim Klerx

Contents

K. Mak (✉) · P. Prah · C. Meurers
National Defence Academy, Ministry of Defence and Sports, Republic of Austria, Vienna, Austria
e-mail: klaus.mak@bmlvs.gv.at; peter.prah@bmlvs.gv.at; christian.meurers@bmlvs.gv.at

J. Göllner
Institute of Strategy, Foresight, Risk and Innovation Management, MASARYK University, Socio-Economic Faculty, Brno, Czech Republic

Center for Risk and Crisis Management, University of Natural Resources and Life Sciences, Vienna, Austria
e-mail: johannes.goellner@bmlvs.gv.at

J. Klerx
Foresight, Research, Technology and Innovation Policy, Austrian Institute of Technology, Vienna, Austria
e-mail: joachim.klerx@ait.ac.at

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_32

Abstract

The handling of Open Source Information in the field of the domain "Cyber" is one of the future challenges for the Central Documentation (CentDoc) of the Austrian National Defence Academy. The CentDoc is responsible for "Open Source Information-Processing" and the Research and Development topic "Documentation and Knowledge Management" of the Austrian Ministry of Defence and Sports. Under the perspective of finding new solutions to develop knowledge and to support decision-making in organizations with relevant, high-quality Open Source Information (OSInfo) and Research and Development products, the "Cyber Documentation and Research Center" ("CDRC") was founded in 2014. This paper will give an overview of the present challenges of OSInfo and new perspectives of solutions to solve current problems and create new ideas. A so-called "High Quality Crowd" and further on a "Crowd Network" will be presented as a new method for crowd OSInfo with a description of goals, organization, processes, and products of the CDRC as a horizon scanning center for cyber security. The surprising results and experiences of this project did challenge not only the traditional working methods but also the required new ways of thinking.

Keywords

Horizon scanning center · Crowd sourcing · Open source intelligence · OSINT · Documentation · Cyber defense · Cyber analysis and monitoring · Situation awareness · CDRC

Introduction

Successful knowledge management in organization always demands for new solutions, new perspectives, and new ways of thinking aside traditional ways and methodologies. The pragmatic understanding of "knowledge" was the precondition for the development of new perspectives, models, methods, and approaches to the "Cyber"-Domain in relation with collecting, analyzing, and visualizing information from heterogeneous, multilingual, and open sources.

Knowledge is therefore the ability to interpret data and information correctly and reproducible, depending on the system's environment. Data and information are in general not sufficient for an interpretation itself, lack of time, deficits like incompleteness or quality issues, and other restrictions limit the quality of the results and determine in further the quality, risks, or the uncertainty of a decision or nondecision. The distinction of implicit and explicit knowledge refers to human skills like experience, language skills, wisdom, etc. on the one hand, and the understanding not only of the organizational know-how, but of the systems context as well, on the other hand. Therefore, the "document" represents a system relevant unit, which consists of data-, text-, image-, or multimedia-content.

The CDRC meets these challenges by a new approach of "Crowd OSInf," applying so-called "Cyber-Recruits" of the military for research tasks. The main objectives are "Open Source Information" ("OSInfo") of the "cyber" domain for the Austrian Armed Forces, NGOs, and possibly partner organizations to support "cyber" research and

development projects for the necessary processing mechanisms of OSInfo. The collaboration platform makes use of the individual skill, abilities, and knowledge of the recruits and benefits the development of linguistic skills as well as the technical skills for the Austrian Armed Forces. A "Network of Experts – Cyber" as well as a "Cyber-Militia" guarantee the access to this knowledge in a long-term perspective. Additionally, special tasks of the Austrian Armed Forces relating to SKKM (SKKM: Staatliches Krisen- und Katastrophenschutzmanagement (Crisis and Disaster Management on a State Level)) or R&D in general as well as fields of economic enterprises, particularly critical infrastructure, can benefit from the expertise of cyber recruits.

Results show the efficiency and effectivity of this crowd-based approach and new implications and findings can be derived regarding societal, security, and military dimensions. With the help of heuristics, these findings are formalized and documented for the system. Close cooperations with research partners like the Austrian Institute of Technology (AIT), partners from KIRAS (KIRAS: http://www.kiras.at (Austrian National Security Research Program)) projects, industry, and universities ensure the scientific quality of the work and help to integrate new developments, approaches, and models to the organization as well as to implement a "HSC (HSC: Horizon Scanning Center) – Cyber," which is also applicable to other domains in the future.

Foresight

The pilot phases of the CDRC have shown that methods such as crowd research and the model of temporal source interdependence for information compression are powerful tools for information spaces for example for the strategical preparation of the cyber space. These methods could significantly improve the availability of information for both government services, as well as for research and industrial development.

Knowledge-intensive products - like a research database "cyber" or a knowledge logistics "cyber" (based on the knowledge logistics models of the CDRC) - contribute to a rapidly developing field (the "cyber domain") and can be reused for a coordinated long-term strategy. After digitization was identified as the most important prospective and strategic field in Germany, methods for dealing with the high speed of innovation as well as a scientific field following the digital revolution are more important than ever.

A continuous horizon scanning results not only in that one is surprised by upcoming news. It makes it possible that the skills of the Horizon-Scanning and digital knowledge management are continuously developed. These skills contribute to having "cyber – situation reports" always available in an updated version. They also contribute to foresight having information about possible long-term developments available when examples are needed in research planning. The following chart summarizes the main elements of the model of temporal source interdependence for information compression of section "Crowd: Association Heuristic" together. The continuous monitoring of the cyber domain allows only a very limited conclusion about trends in cyber space. The inclusion of historical information and Foresight information extends this perspective immensely (Fig. 1).

Without adequate technical support, this extension of perspective is not possible. Methods of text analysis "cyber," the semiautomatic translation, the multilingual

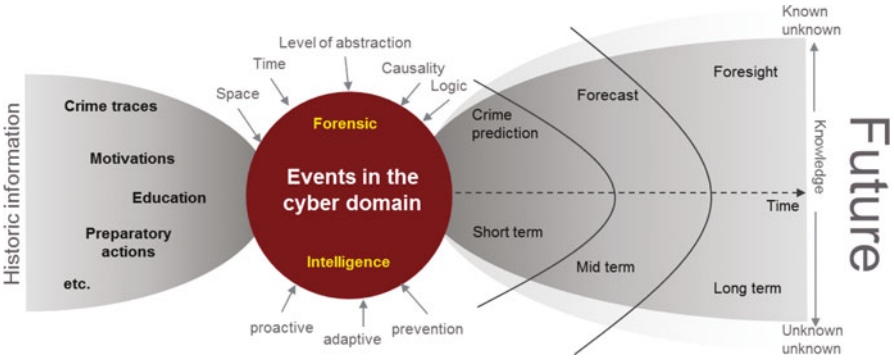


Fig. 1 Meta-logic for development of proactive and adaptive strategies (Source: own figure)

thesauri "cyber," and modern high-performance crawling systems make efficient work of the crowd possible. The development is by no means complete. Many of the current processes need scientific instruments that have yet to be developed.

Until a horizon scanning center can be operated, which fulfils all functions summarized in Fig. 11, it will take some time. However, the current results of the CDRC suggest that the open source analysis and the scientific knowledge management will change with these processes.

All these processes, methodologies, and technologies are integrated and linked in a generic process model for Knowledge Development, the "Z-Model." It follows a comprehensive approach and describes the embedding of foresight as well as the CDRC in an organization's knowledge environment (Klerx et al. 2014, pp. 601–607; Göllner et al. 2015a).

Crowd OSInfo, a New Foresight Method

The evaluation of open sources with the help of groups is not new per se. However, this evaluation has not been backed by an information logistics explicitly formulated, which has been developed to carry close cooperation in time to improve the group performance gradually.

Governmental services as well as scientists and technicians usually work with experts who guarantee the quality of their work performance through their years of training and experience. The success of this process depends on the delivery of performance from the individual expert in any given situation. A quality assurance is possible only via a type of peer review by the judgment of other experts.

In recent years, there has been increased success with integrating knowledge-intensive services automatically either by computers or via computer interfaces of human judgment so that they take over the part of knowledge work, where computers are notoriously bad (semantic interpretation, hermeneutic interpretation, adjudication and establishing, image recognition, classification by subject). Platforms such as GeniusRocket, Mechanical Turk from Amazon, Clickworkers, Cloudcrowd,

CastingWords, blur Group, Whinot, IdeaOffer, NamingForce, SquadHelp, Threadless, 99designs, Crowdspring, Prova, Crowdtap, and many others offer approaches to retrieve the increase of performance from human groups in the context of crowd working (Mashable 2011).

Many of these crowd working approaches are suitable to assist the computer with the difficulty of the content analysis of texts. Therefore, these approaches have also long been used in traditional expression of information management of state services. China uses findings of its citizens who are abroad (Mattis 2015, pp. 540–556). In the Arab context, modern forms of information gathering (Westerman 2004; Sanchez 2015, pp. 429–448) and dissemination will be implemented through Swarmcast (Thedailybeast.com 2014) also in the context of civilian groups that use the Internet. In the US, there is evidence that ideas on HUMINT and OSINT by Crowd at least exist (Stottlemyre 2015). The intention of this publication, in May 2015: "*I suggest did KDM crowdsourcing, separate from Daren Brabham's other types, shoulderstand be professionalized across sectors* ...," says Steven A. Stottlemyre (2015, p. 587), exactly what is occurring in the CDRC already and is documented in this publication.

Ultimately, one must speak of a "highly qualified crowd," which was compared with the conventional ideas of crowds with large numbers of participants. The term "high-quality – or high-performance crowd" could be used here accordingly.

Furthermore, the cultural background of the groups significantly influenced the value of the project. After several research on various topics, it has led to the systematic mapping of the understanding of the group on various subjects. This is reflected in the following diagram of the association heuristic of the CDRC-CROWD.

Crowd: Association Heuristic

Crowd association heuristic forms a basis for understanding how a crowd works. There is evidence that depending on the cultural, linguistic, or personnel composition, the OSInfo results of the crowd differ in terms of quality and quantity. Documentation in the form of an association heuristic has proved to be suitable for verifying and explaining those differences.

In particular, personal factors like individual skills, language, knowledge, interests, personality traits, and time significantly influence when explaining the results of a crowd search. Figure 2 provides a detailed overview of the features for which the results of the crowd researches were decisive.

All above depictured associations occurred more or less distinctively when answering the questions in certain configurations. This documentation can be further developed dynamically in PROMOTE® (Mak and Woitsch 2005) and contributes significantly to quality assurance. After each research, it is possible to check whether any new perspectives have been added on an issue or whether it is necessary to extend the research under previously unrecognized associations which previously have been documented in the matrix. This level of quality has not been reached so far, not even by experts.

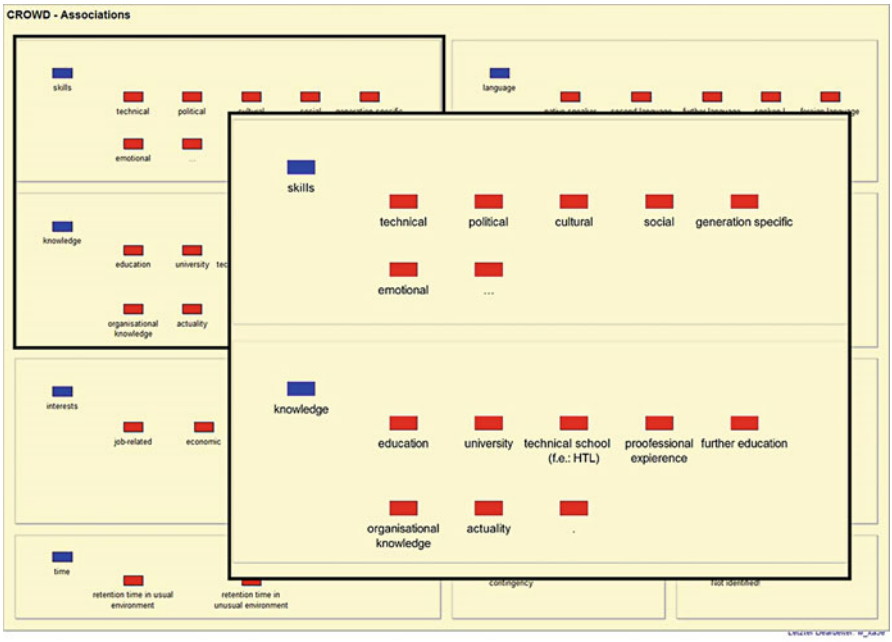


Fig. 2 Overview of crowd association heuristic (Source: own figure)

While analyzing the requests, their variety was systematically taken in to account. More than 300 questions – asked in recent months by all user groups – were analyzed by CentDoc. Likewise, special requirements of the questions in the domain Cyber were documented in this heuristic.

The composition of the crowd can be optimized based on these results. Depending on the query, its topic or objective, and due to factors like time and resources, etc., a specific composition has proven suitable. The aim should be to provide a sufficiently complete research by little efforts. To evaluate the quality of the research, both researches of reference and assessments of experts were used.

CentDoc: Query Heuristic

Another key feature for optimizing a crowd research is the question heuristic. The type of question is a major factor in determining the progress and results of crowd researches. In addition, they provide an overview of user interests and user motivations. The evaluation of the question heuristic allows the quality of the crowd research to improve significantly over time.

Queries can be categorized by, e.g., the nature of the question (questions regarding problems, contexts, existing issues, causes, effects, etc.). This results in open and broad researches with a wide range of possible interpretations for the crowd.

Queries relating to description and explanation of events (who, when, what, where, how, why) often occur in journalistic context. They motivate a specific research, which leads to a structured explanation of an event.

Queries that relate to a certain timeline, such as temporal trend, possible (future) developments, previous developments and explanations, periodic regularities, trends, etc., have proved to be particularly difficult. Especially, the search for future developments requires specific search strategies. The crowd is much more efficient if these search strategies are discussed in advance.

Topic-oriented queries such as crises, conflicts, opportunities and innovations, findings, etc. have similar dynamics as event-related searches have, but are less structured. Depending on the topic, the course taken is quite different. Most topic-classifications can be improved by practice.

The quality of crowd researches on technical queries, such as state of the art, patents, statistics, application-examples, comparisons, and functionality, depends on education and interests of the crowd-research-teams. Search strategies of technically qualified team members differ from those done by team members who are less familiar with technology. However, it has shown that team members taught in linguistics or otherwise enhance the results by applying their unconventional search strategies.

Queries about organization, management, and strategies, such as leadership, plans, roadmaps, implementation procedures, etc., often lead to result-lists which are larger than expected. A quality check done by experts helps to reduce these result-lists.

Queries on relevance of research, with literature researches, program calls, project reports, research institutes, expert networks, MOOCs, development platforms, etc., require specific – but also unconventional – sources. Obviously, on an increasing number of video platforms such as YouTube, relevant results can be found for this segment.

Overall, maintaining query heuristics supports that queries can be asked specific and formulated to the crowd.

When introducing to internet research, search heuristics have proven suitable to explain the range of search methods. Due to the possibility to compare different perspectives on queries with the variety of questions yet achieved options of combinations which had been hardly ever systematically detected and evolve dynamically.

In this form, and combined with support mechanisms such as terminology frameworks, retrieval functionalities, or text analysis tools, they represent a new challenge to the analytical capacity of users. By further S&D work, these mechanisms are better researched and improved processing capabilities in OSInfo area should be created. This represents another focus in the future work of the CentDoc together with its partners (Fig. 3).

Crowd Research

Association heuristics and query heuristics provide the controlled basis to be used by a crowd research team. This chapter presents the detailed workflow of crowd researches and discusses its advantages and disadvantages. No evidence of the use

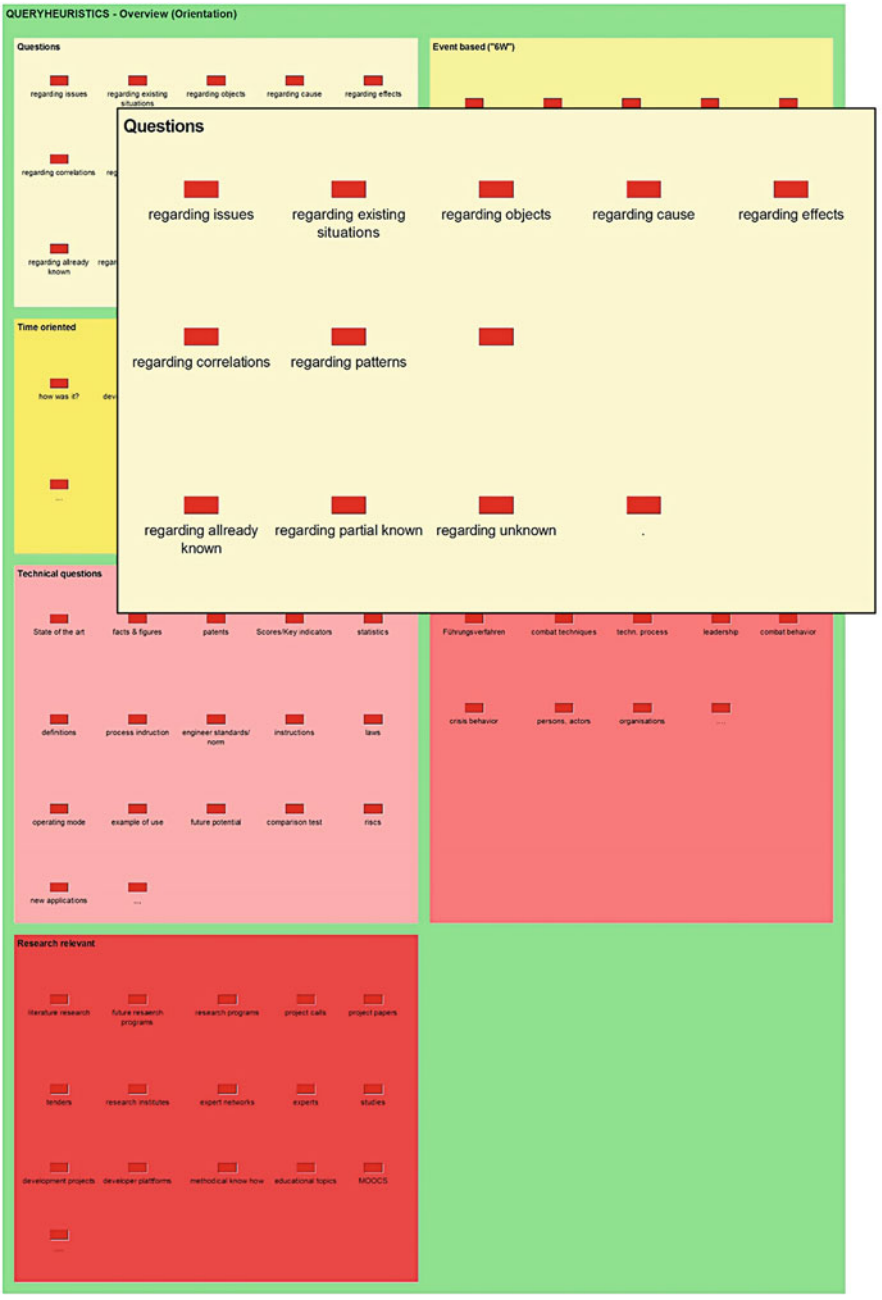


Fig. 3 Overview of the crowd research in question heuristics exemplarily (Source: own figure)

of an organized crowd for research was found in scientific literature, apart from the publications and software developments on crowd working (Mashable.com 2011) and on crowd intelligence (Stottlemyre 2015).

The option of focusing a "high-performance group" ("high-quality crowd" or "high-performance crowd") on a query yielded some surprising results. Due to the high quality of education, the various languages, and wide-ranged associations shown in the matrix, the results were very convincing – not only quantitatively, but so demanding regarding quality and variety that even expert research work could not come close. Also, the time factor became an important criterion, as the group delivered its results 15–20 times faster than a single researcher could have done.

It became obvious that while more and more diverse results were found, the limits of improvement have not been detected yet. The coverage of a question, in order to come to "thorough" results, will be subject to important research in the future.

The crowd researches are supported by generic processes, which had already been featured in the CentDoc and were further developed during the project. Their documentation by process diagrams proved suitable again and saved a lot of training time. The next chapter presents the CDRC crowd research and discusses the experiences regarding its application.

Crowd Research: Generic Process

The crowd research generic process summarizes the key process steps of a crowd research as seen from the perspective of a team member of the crowd. It serves as a basis for training and as a reference for the procedure for each research. This test case is complemented by the knowledge of the crowd heuristics and heuristic questions. Figure 4 provides an overview of the processes.

The process steps of a crowd research consist of setting the search time, the presentation of the preliminary analysis, and the structuring of the topic by the experts of the crowd. During the presentation of the expert, the crowd selects a search strategy and writes it down with the corresponding keywords. Thereafter, the research is assigned to the crowd.

The crowd permanently documents their results during the research and categorizes the results according to the categorization scheme described in section "Cyber: Category System" (example of cyber). After the summarization, evaluation and control by experts, all individual researches are reported via the CDRC reporting system.

With set time limits and search topics, the necessary time correlates with the openness of the topic specification and the type of question. The more precise both are defined, the less time will be needed. However, precise specification subjects lead to less variety in the results. Depending on the problem, this can be an advantage or a disadvantage. Figure 5 shows the first part of the crowd search, until its results are gathered.

The first part of the crowd research process diagram shows how the research order is given to the crowd and how the research is conducted. For the desired level of quality, it is essential that the formulation of the research order is clear and structured for "nonexperts." It has proven advantageous to use the presentation of the prepared

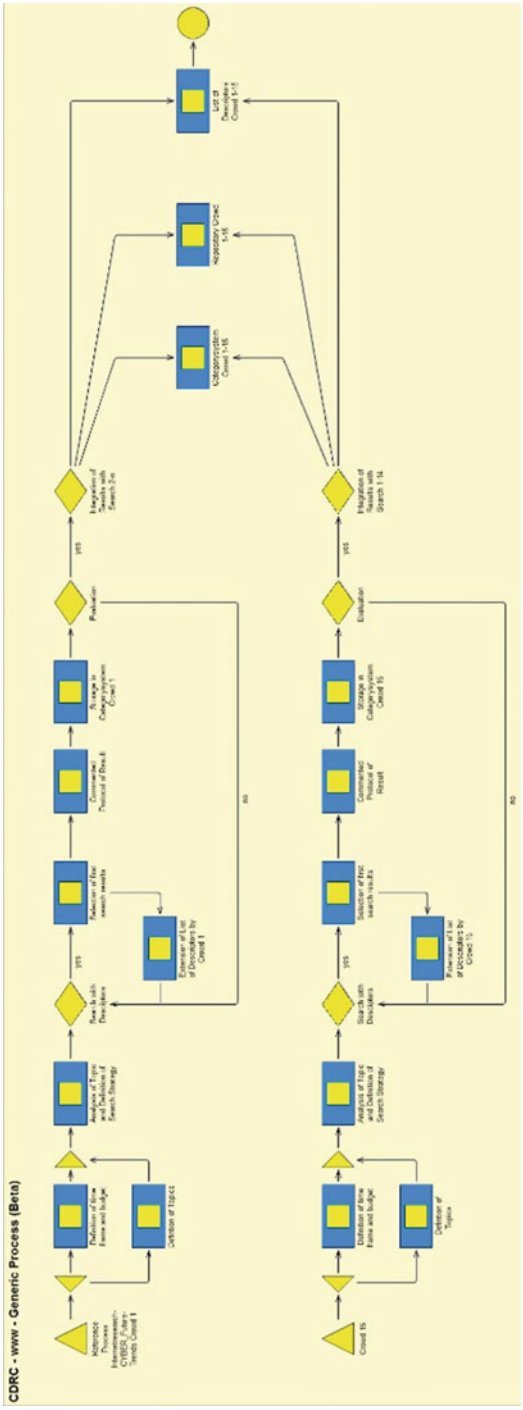


Fig. 4 Process diagram of a crowd research (Source: own figure)

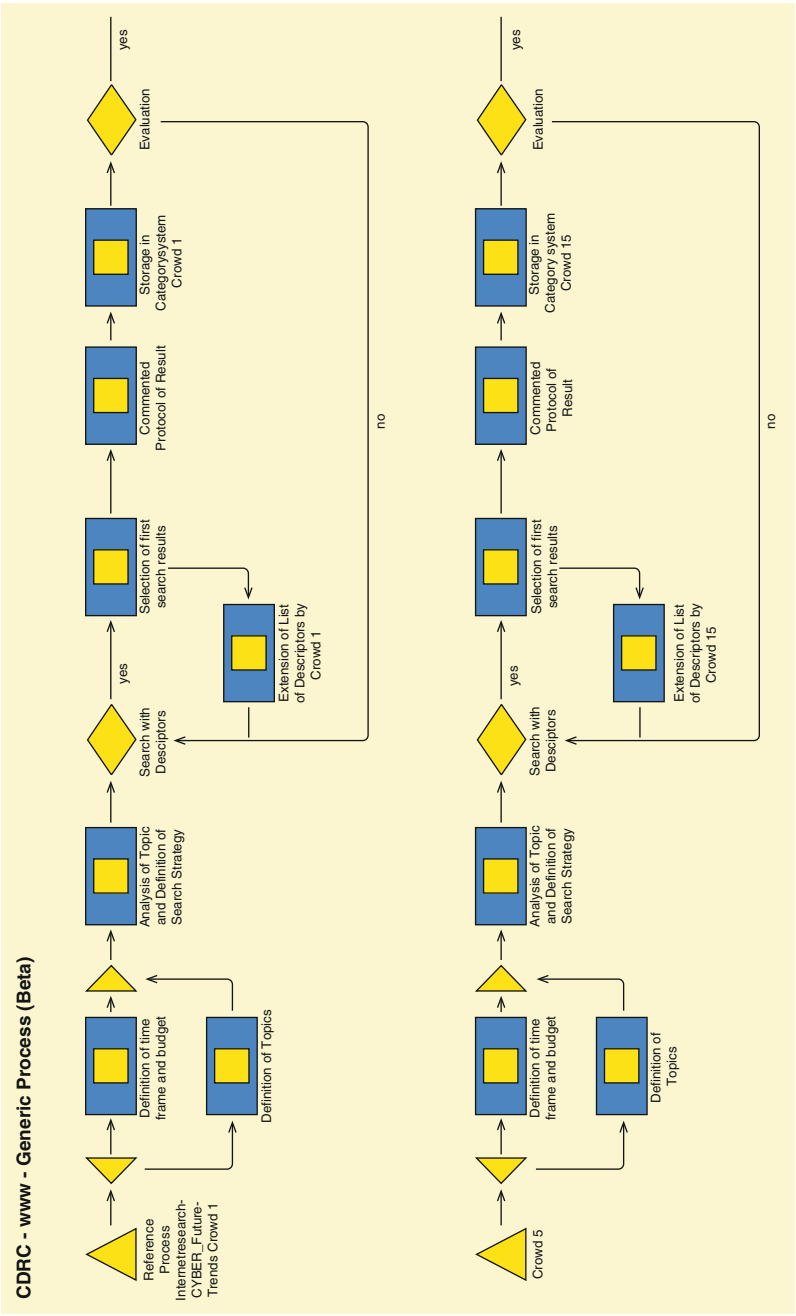


Fig. 5 Process diagram of crowd research part 1: Crowd (Source: own figure)

analysis and topic-structuring done by experts when briefing and introducing the crowd clearly and well-structured to the research-topic. In order to avoid misunderstandings, it is important to include as much background information about occasion and purpose of the research as possible to the crowd at this stage.

The selection and determination of a search strategy is then carried out independently by the crowd. Suggestions for specific search strategies by the experts would limit the association ability of the crowd. Then the crowd receives the order and a certain time limit is set. This limitation should not be too wide, since after a certain time, the testing of new search strategies will become increasingly slower. According to experience, it is advantageous to have already the initial results being reviewed by an expert to prevent misunderstandings and readjust the research direction. The research results are uploaded by the crowd with logging and categorizing according to the CDRC categorization scheme (section "Cyber: Category System") into the CDRC reporting system and are then available for further use.

It became obvious that a second research after the presentation of search results and the search strategies from experts significantly enhances the results of the crowd. The second iteration process of the crowd research is, apart from the additional output information, done in the same way as the first.

In addition to the results of the research, other valuable knowledge products such as a domain-specific category system and domain-specific descriptors lists are created. These need to be merged and adapted from time to time. This process is depicted in the second part of the diagram (Fig. 6).

Since the compilation of the results also provides an overview of the quality achieved, this step is a part of quality management. The aim of quality management in the crowd OSInfo is to ensure the relevance and the accuracy of search results. Information regarding the assessment of relevance must be combined from three levels of opinion. First, the members of the crowd assess each search result, about relevance, correctness, and value for further processing. Then, the experts of the CDRC assess the results of the crowd research. Finally, the client evaluates these results once again. All evaluations contain valuable information for quality assurance and should therefore be documented and saved.

In addition, quite a number of internet services were identified, which allow a direct verification during the research.

There are, for example, still various ways to access web information which are not directly available anymore, such as through search engines caches or the Wayback Machine (archive.org 2015). Individual services can help at detailed and verified researches, such as the citizen evidence lab (citizenevidence.org 2015), which provides instructions regarding the way how to verify information from the internet and offers meta information of YouTube videos.

High-profile sites (HPS) perform a special role when searching for the "most valuable information." HPS have repeatedly shown in searches for various reasons that they are a reliable and valuable source of information. Therefore, they are not only used for quality assurance in CDRC's crowd researches. They are treated separately, regarding their identification, as well as in their processing. This will be described in the following section.

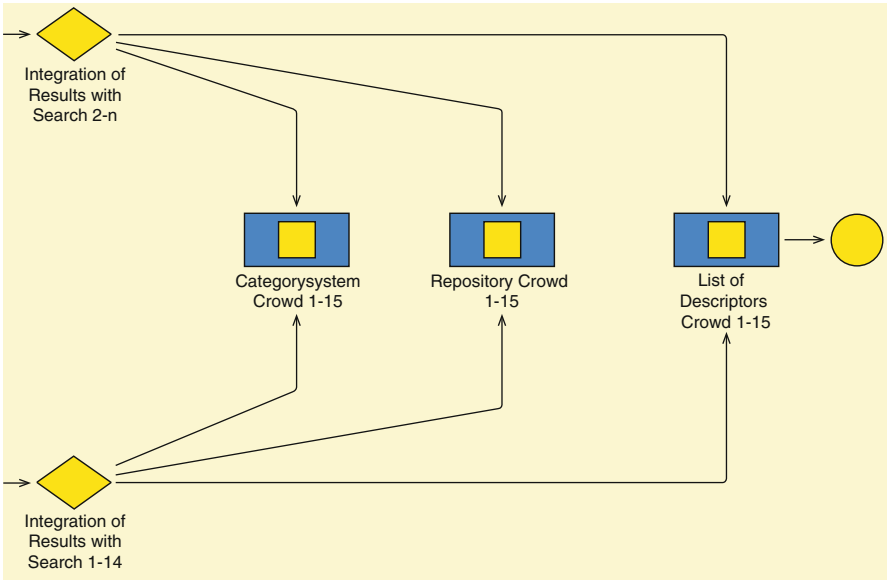


Fig. 6 Process diagram of crowd research part 2: Merging2 (Source: own figure)

High-Profile Sites

The so-called "high-profile sites" (HPS) represent a core element for quality management. These sites include important information about the cyber domain which are evaluated regularly by the cyber recruits. These sites are assessed by the respective internal and external experts according to the criteria shown below, which have been systematically recorded for the first time in this form.

HPS are identified during normal search, or searched and identified in specific researches. In case they are found during other activities of the CDRC, the members of the CDRC will report and process them.

HPS stand out for containing thematically relevant information for the key categories of the CDRC. Furthermore, their information is updated constantly. Often these sites, due to their outstanding quality, have been established as a central hub for a community.

HPS are, e.g., expert sites established in the community with relevant and current conference reports, which are regularly updated, and with platforms, where developers' software and tools are exchanged and updated regularly.

HPS due to content criteria (quality, quantity, timeliness, update frequency) are, e.g., social media platforms, which regularly bring forth new and up-to-date information, such as YouTube channels, expert's Twitter sites, or expert panels.

HPS due to context information on search engines, search tools, terminology tools, and translation services are, e.g., investigative journalism, hacktivism, or other civil society activities in the cyber area.

HPS are used for continuous knowledge accumulation in the CDRC and in crowd researches – not only as a source of content but also for current methodological suggestions.

Crowd Association-Matrix Process ("Opportunities: Threats")

The crowd association matrix is another product for evaluating the crowd research. During the researching activity, an intrinsic knowledge is created about potential opportunities and threats in the cyber area. Therefore, it is natural to try to query this knowledge in its manifest form and with appropriate methods of the crowd and making it visible by doing so. The possibility to comply development and research tasks brought forth various options that have been tested now. The association matrix process shows us a particularly interesting perspective on future potentials for the use of multiple crowds.

The group assessed categorized subjects (such as the internet of things, etc.) about the possibilities to find threats or opportunities (potentials) for security, innovation, or economic benefits in them and rated the subjects on a scale from one to ten. Previously, within the main categories (currently 29), also subcategories were determined, which were then normalized.

In the process depicted below, the single steps are documented and feature detailed information about each methodological requirement. For example, the evaluation algorithm is described in detail. Figure 7 provides an overview about this process.

After an objectification of the results, there is a visualization in a test environment, where particular emphasis was put on topics and subtopics that did not fit into a typical pattern.

All results of these test applications gave cause that the crowd association pattern and the results are to be carefully analyzed of the consequences and further research objects.

For individuals, it does not even appear to be nearly possible to evaluate complex issues and perspectives in this form and visualize new information neither opportunities nor threats. Also, the possibility to understand cause and effect mechanisms must be pointed out as a major advantage of this method.

CDRC Innovation: Model of Temporal Interdependence of Sources for Information Compression

The process of merging the research results of the CDRC is based on a model of temporal interdependence of sources to ensure the quality of information compression (MtIS) in the OSInfo area, which was developed by the CDRC. The challenge to provide open information for a variety of users in a timely manner with high quality demands the CDRC to start the OSInfo analysis on the following three main levels:

1. domain security (mil, CIMIC)
2. research and innovation
3. technology (state of the art for cyber)

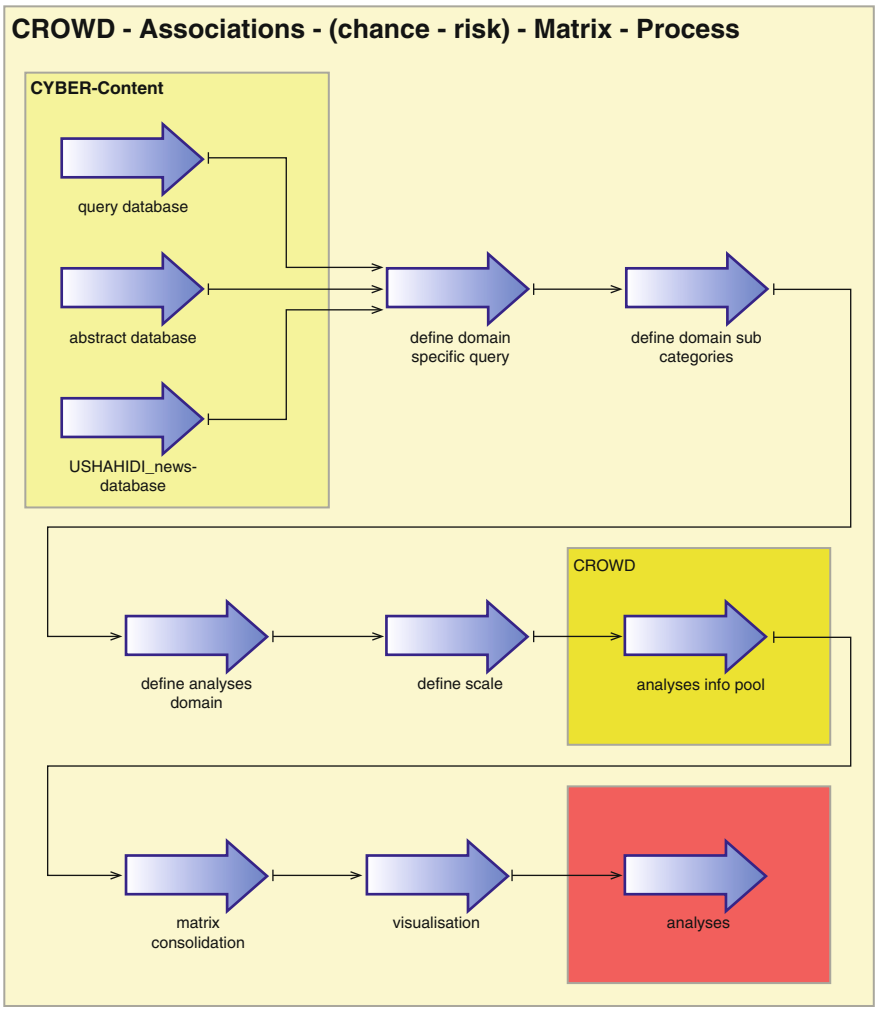


Fig. 7 CROWD – association-matrix process ("opportunities – threats") (Source: own figure)

All contents of OSInfo analyses are additionally used to generate different layer patterns. Real-time situation reports as well as operational situation reports, but also operative strategic location reports or foresight reports, are enriched with open information or processed therein.

During determining the types of documents ("DocType") of Crowd OSInfo researches, it was noticed that different types of information can be arranged in a timeline quantitatively and qualitatively in order to derive time-consistent developments.

This experience in the crowd OSInfo analysis led to developing the model of temporal sources interdependence shown in the Fig. 8. If the information can contribute from different sources at different times to explain events, this knowledge

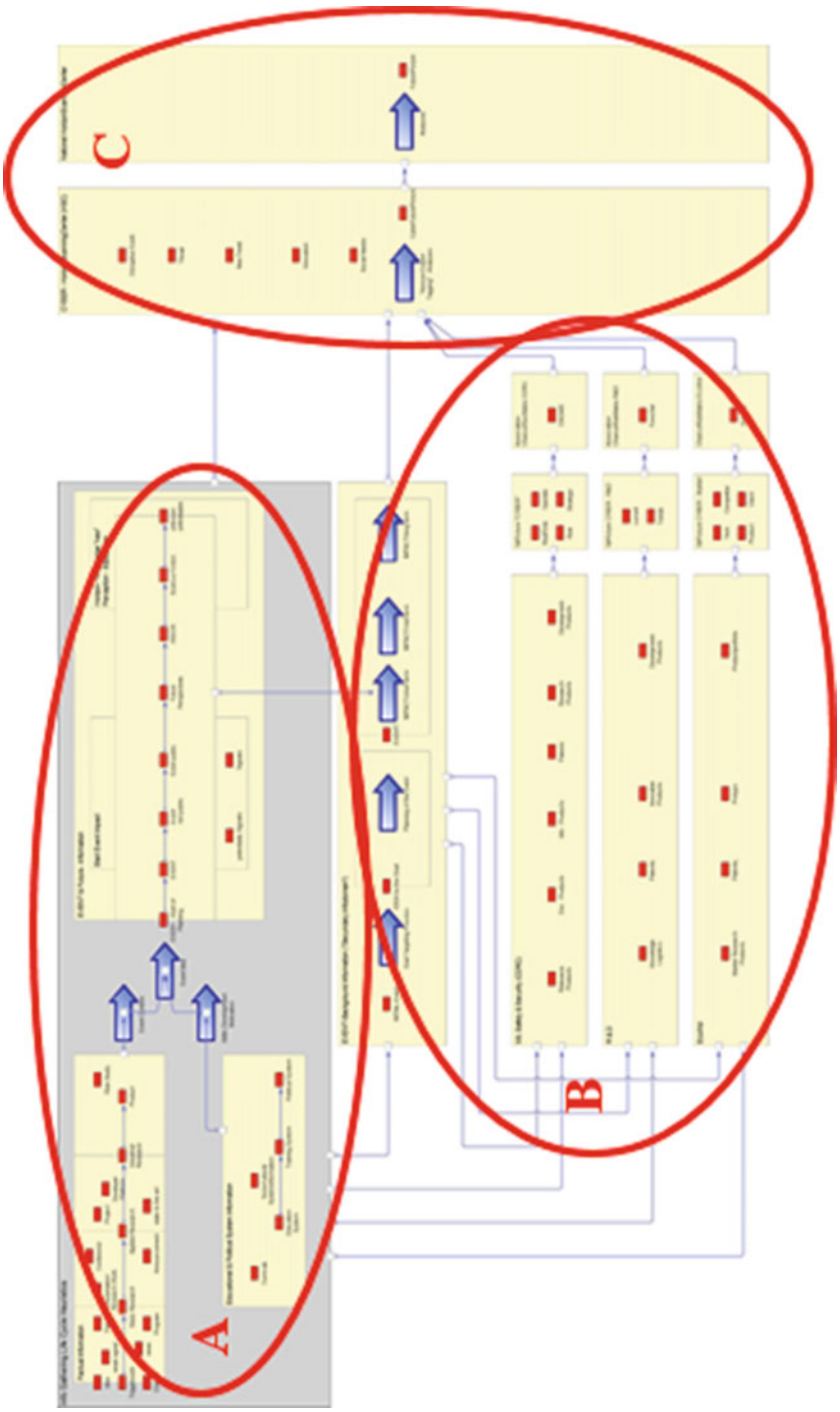


Fig. 8 Model of the temporal interdependence of sources for information compression (Source: own figure)

can contribute as a basis for a better and especially earlier recognition and understanding of new developments.

In order to use this knowledge, it is necessary to structure the relevant knowledge space in a very special way. Assuming an event as the starting point for the temporal assignment of content, the event's history can be traced already while assigning the respective "doctypes" during relevance monitoring. This factual information of the cyber domain enables analyzing the speeds of development. How long is the timespan from a patent to a product? How long does it take for a product to be used in a relevant event? This time factor is crucial in the cyber domain.

Therefore, in the phase model of information gathering, all knowledge objects were arranged in a way that they are, roughly, in a temporal relationship. The segments education and political systems from the information gathering have a special status and have therefore been taken out, as well as the segment of events and future information.

As can be seen in the depiction, all knowledge objects affect the course of an event in their specific way at a particular time. The focus is on the event context, event ideas, and development of capabilities.

In the central area of the model, this is visualized as an effect layer of events. "A" diagram shows an extensive viewpoint of an event as an overview over a key event and its surrounding dependencies.

The immediate, short- and long-term effects of the events, along with the potential signals and the first public appearance, are all essential parts for the future opportunities and threats. Future studies, science fiction ideas, and similar support the view into future.

Likewise, the possibility of categorization of educational and training content shows who is able to implement certain events. Will an individual ever get the chance to obtain certain skills or can certain things only be done by a group? In diagram "B," the secondary information is presented, which occurs around an event. With this secondary information, events can be explained, planning of events derived, motivations identified, effects assessed, and ultimately "Situation Overview" information derived.

A central factor in it is the motivation of the actors of an event. Which actor(s) can have interest in certain things depending on the actor's environment? Ethnic or political, economic, or curiosity-related motives can be found again more easily via evolving patterns after a certain time. This form of information gathering and structuring forms the prerequisite for an effective analysis. Supported by the findings of the association heuristic, it has become possible to make motivation hints lastingly visible. Here, the role of crowd associations deserves special attention and scientific questions are highly relevant as well. In the future, a systematic detection of weak signals must be planned.

The "C" diagram of temporal sources interdependency clearly points out how this information can be used for a comprehensive analysis of events for horizon scanning.

By the event background, the planning and training documents, the motivations, the interests, the ability developments, expectations for the future, the strategy

documents and visions, and new and yet unknown events can be recognized during their origination.

Evaluated by different experts or groups of experts, users of the CDRC can thus rely on up-to-date and comprehensive information which is enriched daily from quality assured sources. The partner phase model, which was developed by the CentDoc in cooperation with the AIT, also illustrates in detail how time and content aspects become basis for an event history. Cause and effect should and must remain recognizable. Otherwise, unwanted effects can never be detected and prevented in their cause.

Cyber Information Platforms

To meet all the requirements of categorization, structuring, metadata capture, typification, and timeliness and make them visible and accessible for the user, different information platforms were evaluated and some modules were developed to an own information platform. Among others, a so-called "Cyber – Ushahidi – information platform" was mounted and put into operation. With these criteria, a quick insight into the "today's current events" can be provided in the cyber domain. When compared to the work of the crowd, the quality of the results of the automated procedure did not even come close. Neither the classification nor the typification and certainly not the recognition of any important additional information on a site ("site info") nor of new contexts was possible to be delivered by a so-called "Crawler."

Figure 9 shows the home page of the CDRC cyber information platform, which was implemented based on Ushahidi.

All administrative and operational requirements of the open source worldwide used platform "Ushahidi" were fulfilled by staff and recruits of the CentDoc. Readjustments of the system during the first year of operation did not raise a problem.

Ushahidi provides a system, developed to meet the requirements of crowd sourcing in the event of a crisis. By adjustments at the CDRC, it is also suitable to serve as a reporting system in the cyber domain, which provides even some simple forms to visualize the results.

The main advantages of having chosen Ushahidi is: messages can be categorized and incorporated into the information system. This message can be assigned to one of the sources' document types (doctype), Furthermore, site information and other metadata can be attached to each message. Besides that, it is possible to implement Expert Tagging into the system. All these elements are necessary to provide information from the cyber domain, according to the monitoring concept of the CDRC and derived from the model of temporal sources interdependency, to ensure the quality of the information compression in the OSInfo area (MtIS).

Categorized by subject and doctype, it is possible to point out first temporal relationships between different doctypes on the Ushahidi platform.

Fig. 9 Home page of the CDRC cyber information platform (Source screenshot: CDRC information platform)

The system of CDRC’s categorization, the CDRC doctypes, and the various forms of metadata in the information management process of the CDRC are depicted below.

Cyber: Category System

The cyber category system of the CDRC serves to roughly cluster the message’s content already when being reported to the system. So, a user can filter messages by category to observe and assess only messages from specific individual categories. If a cyber-expert is only interested in, e.g., methods of attack from the technical perspective, he can hide all other messages and only get these from the system.

As depictured in Fig. 10, there are currently 29 categories to classify messages.

These categories developed during daily work and are subject to a constant conversion and improvement process. New categories can be added whenever needed during crowd research, especially of HPS and can be deleted if there are no or not enough assignable messages for the category.

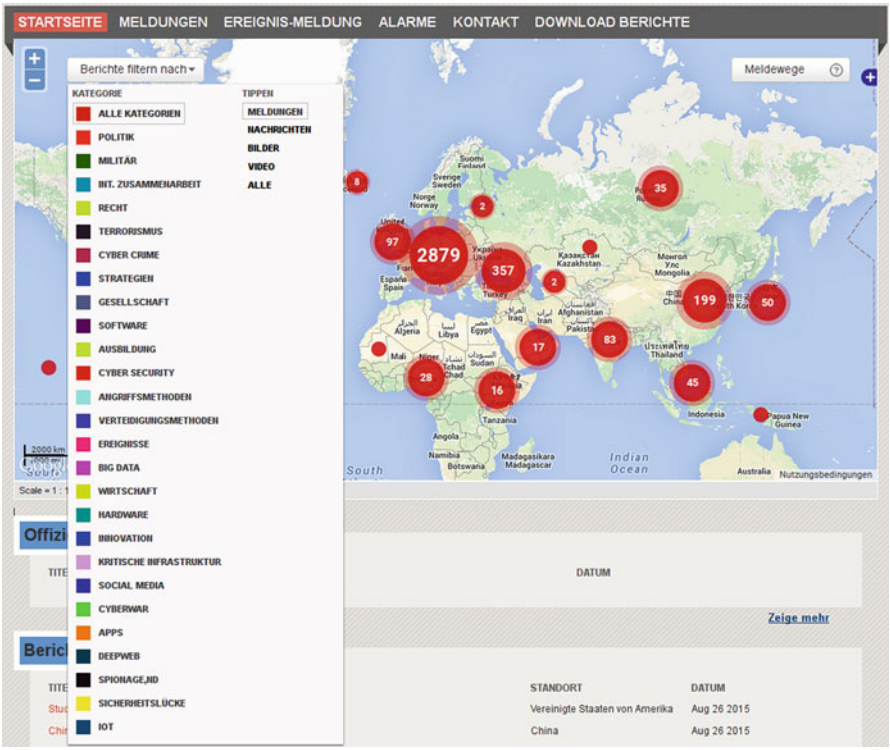


Fig. 10 Category system of the CDRC cyber information platform (Source screenshot: CDRC information platform)

By now, the category system has "stabilized," and such changes have become increasingly seldom. Nevertheless, the categories must keep proving their usefulness to the user. User statistics will show which categories are needed more than others. By adapting the information system, it will be increasingly easier to use and therefore more valuable to users.

Horizon Scanning Center "CYBER"

In recent years, a growing number of horizon scanning centers (HSCs) have been set up to provide information which supports government institutions in long-term planning. The aim of HSCs is to collect all relevant planning information for a particular domain as early and completely as possible and to have it reviewed by experts.

A description of HSCs in Singapore, the Netherlands, at the UN, and in the EU was published in "Knowledge Management in the Austrian Armed Forces – Foresight for strategic long-term planning" by the Austrian Defence Academy (Göllner et al. 2015b) (Fig. 11).

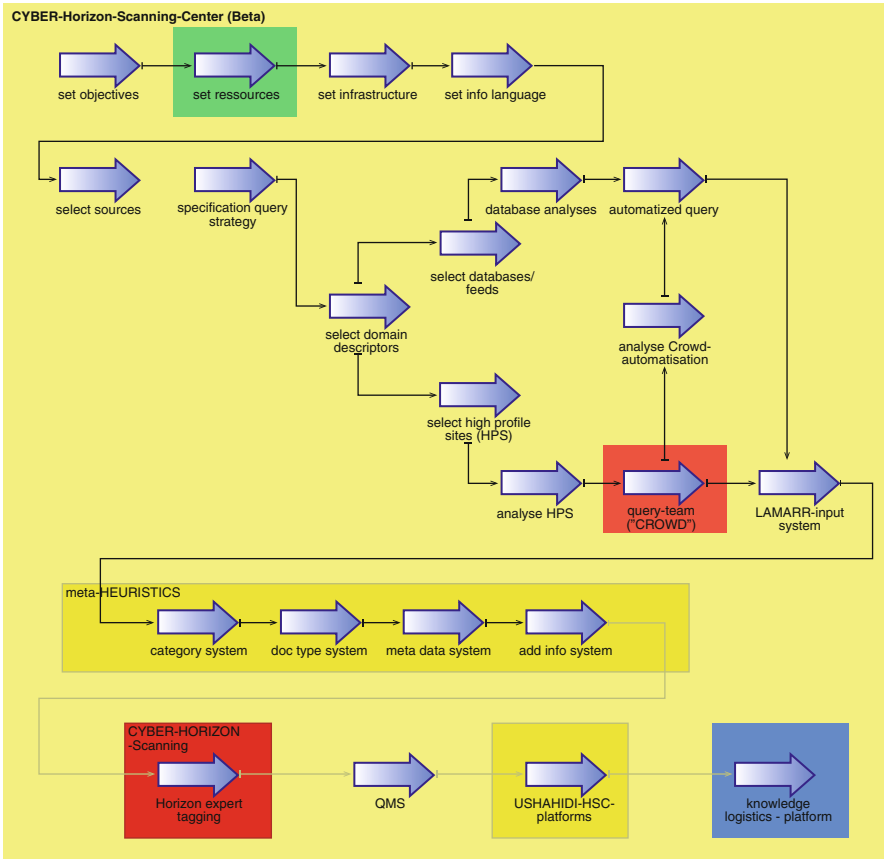


Fig. 11 Process diagram of a horizon scanning center (Source: own figure)

Depicted above is a process diagram which illustrates the processing steps which are necessary to establish a "horizon scanning" for the cyber domain. In this first determination, all benefits of working with the crowd have been implemented in the entire system. To combine it with quality-assured automated information extraction methods will be a further challenge, especially for hybrid and multilingual information elements such as videos and social media. All options for developing further, also for other domains, can be collected systematically, tested, and upgraded.

After defining resources, necessary infrastructures, and relevant languages, it is crucial for any horizon scanning to select the sources and the search strategies. Both should be done in an iterative process, so that both the source selection and the search strategy will improve over time.

Besides the sources of the Crowd OSInfo analysis, the expert research requires descriptors, databases, and feeds. The interaction of the two research methods results in getting a first situation overview.

While questioning at this point the current level of automation, durable analyses must be done on found information, analyses which contribute to future scenarios of the HSC (depending on its tasks or intention).

Such scenarios represent comprehensible future expectations which are transparently justified and rated, to ensure that any occurring change in knowledge will lead to appropriate changes of scenarios. Any future assessments, such as desirable and undesirable scenarios, possible threats, possible disruptive events, possible extreme events, and possible trends, will – as far as possible and appropriate – be rated in probability and impact indicators in order to enable risk analyses.

Continuous preparation and processing will help to respond quickly in individual cases, even at the occurrence of unexpected events. However, the ability of enhanced resilience bears the considerable costs for continuous horizon scanning. The general benefit for a government is the reduced uncertainty among potential future developments, enabling it to better planning and better preparation regarding undesirable developments.

Already now, Austria's CDRC has repeatedly led to certain benefits for the state. The pace of innovation in the cyber area is simply too high for classic training, research, and teaching mechanisms to cope with. Using the methods of the CDRC, both the members of the crowd sourcing as well as the experts will achieve a completely new perspective on developments in the cyber area. The methods to define a state of the art at any given time have changed enduringly due to the innovations of the CDRC. Expert researches without the assistance of a crowd research are simply of poorer quality, so complementary crowd researches will most probably be used increasingly often.

With the methodological innovations in the CDRC, it will be easier to keeping up with the pace of innovation in the cyber domain. This is the experience shared by all stakeholders of the CDRC pilot project.

Future Perspectives

Even if the first steps in keeping the pace of innovation in the cyber domain were successful by using our new methods, it is very clear that many innovations will be needed to stabilize these results. With adequate technical solutions, the analytical capabilities can be optimized. Without these solutions, at some point, the information flow will be faster than the corresponding analytical capabilities. Thus, there is a need for new data mining methods in the cyber domain.

Therefore, R&D activities are provided for the following:

- modern high-performance crawling systems, which would make the crowd more efficient
- automatic text analyses, with topic mining and emotion mining
- semiautomatic translation with the creation of multilingual thesauri
- big data demonstrators for high-performance "cyber" crawling systems
- process innovation with a new and enhanced "crowd research model"
- a "crowd-evaluation model"

The development is by no means complete. Many of the current processes need scientific instruments that have yet to be developed.

To a full-fledged operational horizon scanning center for cyber security, it is a long way to go. However, the current results of the CDRC suggest that the open source analysis and the scientific knowledge management did produce promising results, so that it is worthwhile to go on.

Cross-References

► Concept for Strategic Foresight Knowledge Development Framework for Horizon Scanning Center

References

Archive.org. (2015). http://archive.org/web/. 23 Sept 2015.

Citizenevidence.org. (2015). http://citizenevidence.org. 23 Sept 2015.

Göllner, J., Klerx, J., & Mak, K. (2015a). Wissensmanagement im ÖBH – Foresight in der strategischen Langfristplanung, Schriftenreihe der Landesverteidigungsakademie, 5/2015, Vienna, 2015.

Göllner, J., Klerx, J., & Mak, K. (2015b). Knowledge development and horizon scanning for strategic longterm planning in cyber security. *Security and Defence Quarterly, 2*(7), 5.

Klerx, J., Göllner, J., & Mak, K. (2014). Horizon Scanning for emerging risks in supply chain systems. In *Wilby, Blachfellner, Hofkirchner, Book of Abstracts, EMCSR-European Meetings on Cybernetics and Systems Research*, Vienna, 2014.

Mak, K., & Woitsch, R. (2005). Der Einsatz des prozessorientierten WM-Werkzeuges PROMOTE in der ZentDok der LVAk, Schriftenreihe der Landesverteidigungsakademie, 19/2005, Vienna, 2005.

Mashable. (2011). http://mashable.com/2011/04/01/make-money-crowdworking/. 8 Sept 2015.

Mattis, P. L. (2015). Li Kenong and the practice of Chinese intelligence. *International Journal of Intelligence and CounterIntelligence, 28*(3), 540.

Sanchez, S. E. (2015). Spider web: Al-Qaeda's link to the intelligence agencies of the major powers. *International Journal of Intelligence and CounterIntelligence, 28*(3), 429.

Stottlemyre, S. A. (2015). HUMINT, OSINT, or something new? Defining crowdsourced intelligence. *International Journal of Intelligence and CounterIntelligence, 28*(3), 578.

Thedailybeast.com. (2014). http://www.thedailybeast.com/articles/2014/10/01/isis-is-winning-the-online-jihad-against-the-west.html. 23 Sept 2015.

Westerman, T. (2004). TERROR GOES ANALYTICAL – AL QAEDA IS WATCHING, Same Hatred, New Approach, looking for Weakness, and No Apologies, March 26, 2004, International News Analysis Today. http://inatoday.com/terror%20goes%20analytical%20032604.htm. 8 Sept 2015.

Global Supply Chain Network Risk Analysis and Monitoring for Global Cyber-Defense

41

Johannes Göllner, Andreas Peer, Stefan Rass, Gerald Quirchmayr, and Viliam Zathurecky

Contents

J. Göllner (✉)
Institute of Strategy, Foresight, Risk and Innovation Management, MASARYK University, Socio-Economic Faculty, Brno, Czech Republic

Center for Risk and Crisis Management, University of Natural Resources and Life Sciences, Vienna, Austria
e-mail: johannes.goellner@econ.muni.cz; johannes.goellner@zfrk.org

A. Peer
Center for Risk and Crisis Management, Vienna, Austria

M2D MasterMind Development GmbH, Vienna, Austria
e-mail: andreas.peer@master-minde.at; andreas.peer@zfrk.org

S. Rass
System Security Research Group, Institute of Applied Informatics, Universität Klagenfurt, Klagenfurt, Austria
e-mail: stefan.rass@aau.at

G. Quirchmayr
Faculty of Computer Science, Research Group Multimedia Information Systems, University of Vienna, Vienna, Austria
e-mail: gerald.quirchmayr@univie.ac.at

V. Zathurecky
Institute of Strategy, Foresight, Risk and Innovation Management, MASARYK University, Socio-Economic Faculty, Brno, Czech Republic
e-mail: viliam.zathurecky@econ.muni.cz

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_33

Abstract

The importance of integrated risk management of supply chains is increasing as well as the dependence of critical or strategic infrastructures. Especially, the dependence of energy supply and the information and communication technologies increases rapidly. On the other hand, new threats like Cyber threats occurred. Therefore, the existing risk-management systems fall too short and cannot match the existing complexity.

Within this publication, there are some necessary steps explained for the development of an integrated supply chain risk monitoring and supply chain risk rating model. The basis is a standardized categorization system, and then the red thread is explained with a bottom-up process.

The goals are to develop an integrated risk monitoring and risk rating model for defined clusters as well as for the supply chain as a whole and the description of a supply chain network risk monitoring system as well as a supply chain network risk rating system. The background of these considerations is the improvement of the strategic and operational decision-making process via innovative systems and models.

Keywords

Risk rating · Risk monitoring · Supply chain · Supply chain networks · Generic model · Categorization model · Risk management · Cyber threat · Cyber security · Information and communication technology infrastructure · Energy supply infrastructure · Critical infrastructure · Supply chain risk management

Introduction

Over the past decade, the awareness of the importance of risk management for supply chains has risen continuously (Risk Management Association e.v. 2015, p. 4). Recent incident, such as the catastrophic floods in the Bangkok region in 2011 (BKK 2011), have demonstrated the high interdependency of international supply chains, in this special case the high dependence of the worldwide hardware industry on disks manufactured in the flooded region. This and other similarly disastrous events have led to a renewed interest in robustness and resilience of supply chains (Wilding 2011). Also, the various cyber threats continuously increase and the number of attackers (states or professional criminals) capable of developing cyber attacks is increasing (CCN-CERT 2016; North Atlantic Treaty Organization 2013, p. 24).

The need of an integrated supply chain risk management is supported by the complex situation the acteurs are confronted like (Goellner et al. 2014b; Risk Management Association e.v. 2015, pp. 7–8):

- globalization
- specialization
- homogeneity of strategies and business models
- outsourcing
- competition
- fusion of IT and production in and between companies
- corporate social responsibility and compliance

The Allianz Risk Barometer 2016 shows the change from the normal risks like natural hazards or floods to the new risks like cyber risk, competition in market developments, or multi-incidents. The complete result is shown in Fig. 1. Amazing is that the second and third events, also the cyber incidents, are totally new on the list for 2016.

Under the aspect of industry 4.0, the topic of cyber threats also increasing immediately and security especially cyber security is a "moving target," accordingly the threats must be evaluated continually (Plattform Industrie 4.0 2015, p. 74).

Also, the future energy supply mainly depends on information and communication technology systems (Goellner et al. 2014a).

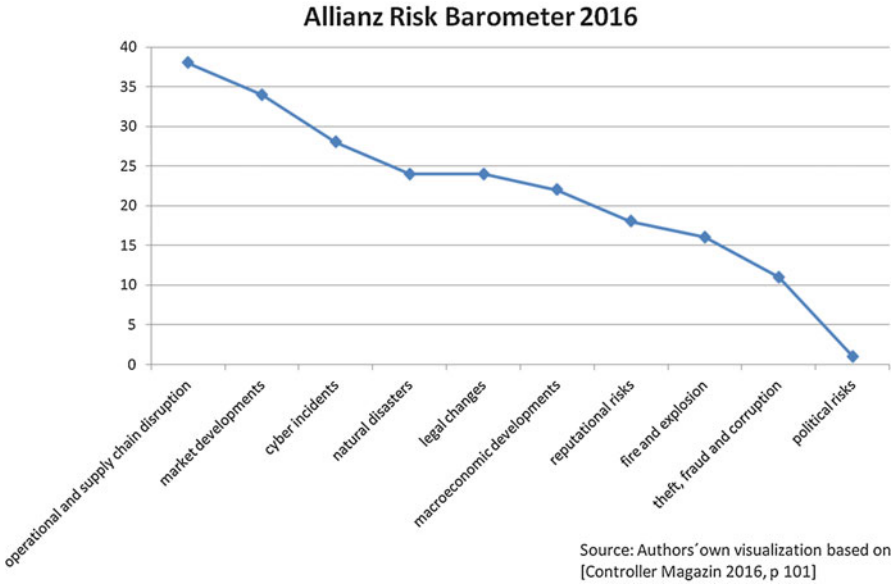


Fig. 1 Allianz Risk Barometer 2016 (Source: Authors' own visualization based on Controller Magazin (2016), p. 101)

Generally, all critical infrastructures are highly interconnected and mutually dependent in complex ways, physically and through information and communication technologies (so-called "cyber-based systems") (Rinaldi et al. 2001, pp. 11–25).

In the innovative field of logistics, there are also a lot of trend analysis, future pictures, and studies available. On the other hand, the "threat side of the supply chain security equation," including also exogenous threats to the EU, is not well covered within literature. Terrorism threat and cargo crime is given great importance. At least this applies in the first decade of the twenty-first century (Cross-border Research Association 2012, p. 99; North Atlantic Treaty Organization 2015).

Within the Deutsche Post DHL "*Logistics 2050*" scenario process based on input from internal logistics experts of Deutsche Post DHL and renowned external experts from diverse fields, a total of five scenarios were developed. Since the focus rests not only on the possible future environment but also on the implications taken from the scenarios, they are the method of choice for reflections on long-term-oriented strategies and policy measures (Deutsche Post AG 2012, pp. 14–17 and 34). In four scenarios, the key takeaways for the logistic industry being shaped by specific heavy weights but always based on innovative and smart logistic solutions. Some of the conclusions are:

> In some parts of the world the last mile delivery network is also maintained as a backup service for communication in case online systems fail. (Deutsche Post AG 2012, p. 109)

> The production process for most goods changes dramatically. A significant share of households is equipped with 3D printers. Many people produce smaller, less complex items and products at home. Construction blueprints for these products are either self-designed or bought in online shops. (Deutsche Post AG 2012, p. 81)

> Daily deliveries within city regions are carried out by electric vehicles with fuel cells or battery packs. (Deutsche Post AG 2012, p. 65)

> Manufacturers increasingly outsource their logistics needs, as logistics providers are capable of planning and controlling the respective processes more efficiently. (Deutsche Post AG 2012, p. 50)

A very innovative logistic initiative which are right now is taking place under funding from the European Union Seventh Framework Programme, which started in 2012, is MODULUSHCA – "Modular Logistics Units in Shared Co-Modal Networks." MODULUSHCA is about a new concept for logistics operations. The project addresses the recently introduced Physical Internet vision (PI), which proposes to use a new framework of interconnected logistics especially designed for open resource sharing, notably thanks to open standard on load units, real-time identification and routing through open facilities (modulushca 2016 June 25). Another innovative logistic project called QUICKWAY deals with an innovative traffic system for future cities (TU Graz 2016 July 02).

So, the identification of potential risks is important for all phases of an event to fulfill the relevant parameters of the strategic and also the operational risk management. For these relevant phases, there is a well-known common three-phase model

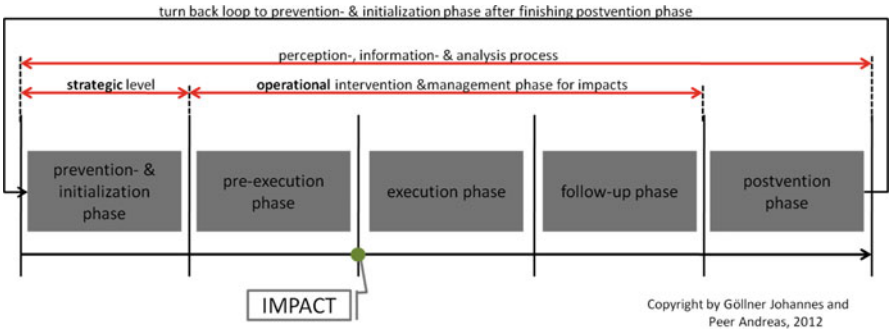


Fig. 2 Five-phase model for crisis management (Copyright by Göllner and Peer 2012)

of the crisis management or business continue management can be expanded by two additional phases, the prevention and initialization phase as well as the postvention phase. These additional phases allow a feedback-cycle of planning, control, and development activities integrating the results, experiences, and lessons learned from the postvention phase. The so-called "*5-phase-model for crisis management*" is shown in Fig. 2 (Backfried et al. 2013, 2016, pp. 469–487; Peer et al. 2014b).

Consequently, society and economy, i.e., enterprises, governments, NGOs, and individuals, have to address a wide range of issues:

- the development of a robust and standardized interaction mechanism for controlling increasingly complex and interdependent supply chain networks (Wilding 2011)
- the relation between global, supranational, regional, and local supply relevance and density under resilient conditions (Buzan and Waever 2003, pp. 445–455)
- the prediction and anticipation of potential disruptions of centralized and decentralized supply chain networks in relation to potential events, space, time, and level of abstraction in order to design adequate avoidance and mitigation strategies, and emergency plans both for the public and the private sector based on accumulated knowledge and empirical best-practices (Goellner et al. 2010d, 2014a; KIRAS 2013a, pp. 21–24)
- the provision of robust and reliable communication and logistics for all involved stakeholders, especially for the purpose of adequate status information (Goellner et al. 2011; Peer et al. 2014a)

For example, some of the identified aspects were picked up in the special Working Group Supply Chain Risk Management initialized from the Risk Management Association e.V. with the aim to develop a guideline for Supply Chain Risk Management (Risk Management Association e.v. 2015).

Advanced concepts for future risk analysis of supply chains should therefore support and improve the above issues, which sometimes need to be done in ways not anticipated before. Risk analysis concepts, models, and methods should ideally

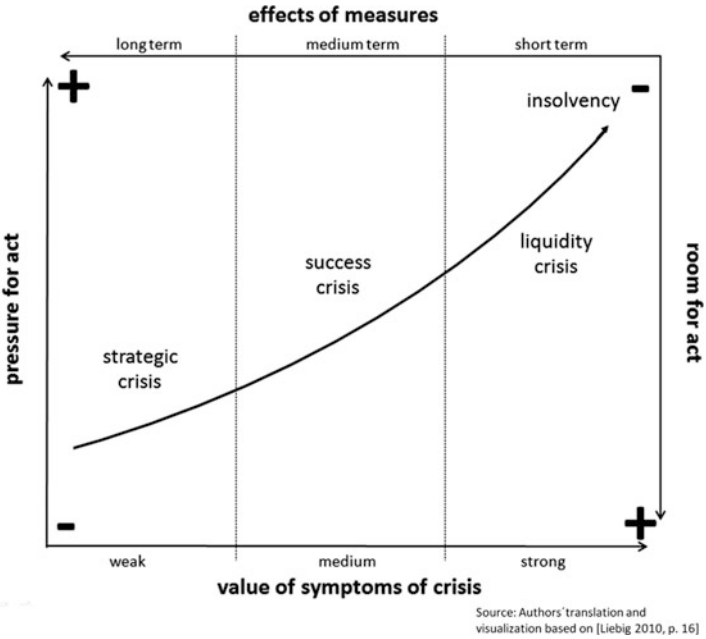


Fig. 3 Four-phase model for Müller (Source: Authors' translation and visualization based on Liebig (2010), p. 16)

allow for the speedy aggregation and presentation of data, information, and knowledge supported by effective and efficient communications in new ways, offering improved interpretation, assessment, and decisions.

Ultimately thereby are also appropriate strategic early warning systems available. This is particularly relevant in terms of corporate crises. In the crisis over the scope of the present crisis, phase decreases as illustrated in Fig. 3.

Especially in the beginning of an existent-threatening crisis, also in the strategic phase, the values of the symptoms are weak. Therefore, risk rating and risk monitoring systems are essential elements of the necessary early warning systems to ensure less pressure and a maximum of room for acting for decision makers.

Identification and Systematization

The first step is to do the identification and systematization work. With the so-called "*Multi-layer Multiple Vector Model,*" this is possible in a standardized way.

The "*Multi-layer Multiple Vector Model*" represents a three-dimensional, multi-level meta-classification system in which each element can be shown and described on the vektorale assignment of defined properties and attributes (Goellner et al. 2014a;

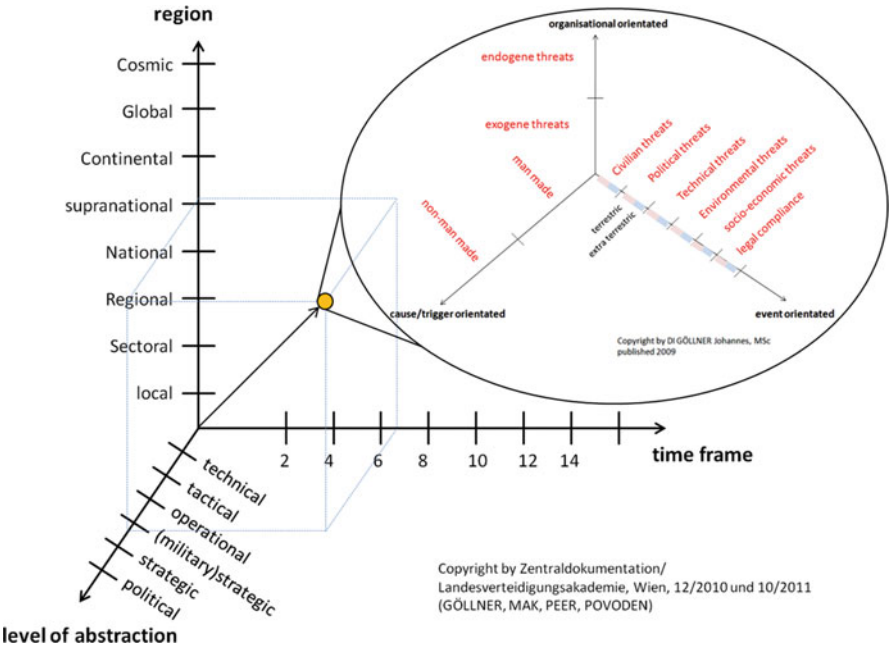


Fig. 4 "Multi-layer Multiple Vector Model" (Copyright by Zentraldokumentation/Landesverteidigungsakademie, Wien, 12/2010 und 10/2011 (GÖLLNER, MAK, PEER, POVODEN)

Backfried et al. 2016, pp. 469–487). The Model based on six axes in two layers which are designated as

- region
- level of abstraction
- time frame

in layer one and in layer two are the axes designated as

- organizational orientated
- cause/trigger orientated
- event orientated

Even the distinction between terrestrial and extraterrestrial mapping is possible. So, everything happens may categorized in a standardized and structured way (Fig. 4).

The main topic is to follow an integrated approach consisting in the core of contributions from logistics, risk analysis, performance management, and information and communication technology including the human factor. Under this approach, the structured basis divides the following segments:

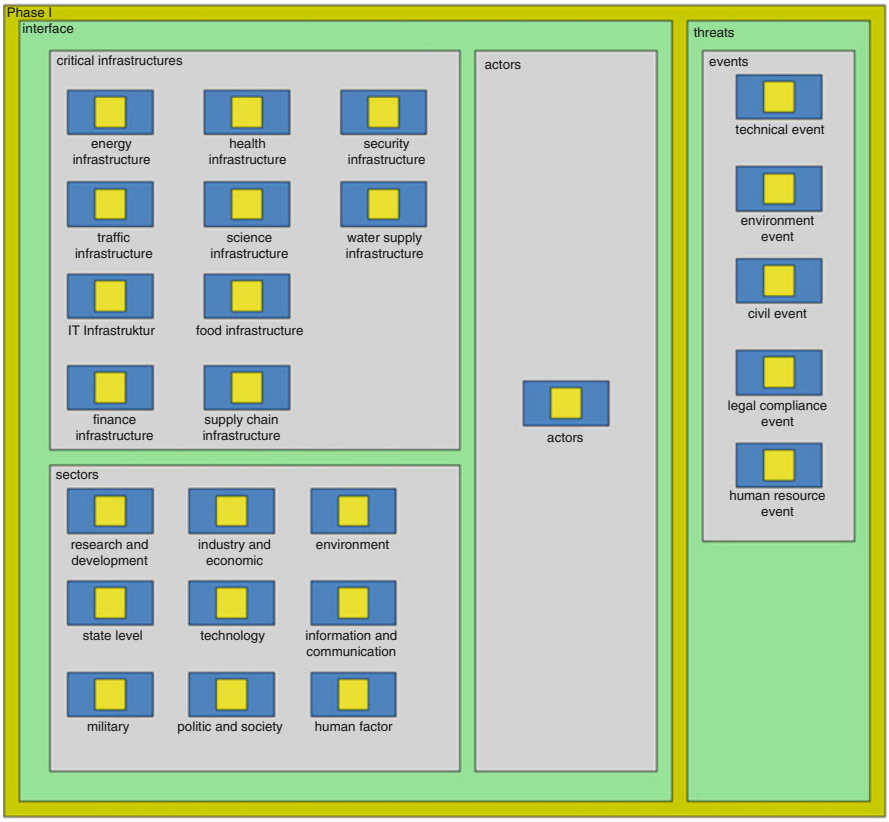


Fig. 5 Structure and interface for comprehensive risk analysis (Copyright by Göllner and Peer 2012)

- critical infrastructures
- sectors
- actors
- events

The interfaces of the first three segments combined with the possible threats are the basis of an integrated risk analysis (Peer 2004; Buzan et al. 1998; Vester 2008; Poustourli and Kourti 2014; North Atlantic Treaty Organization 2013, pp. 43–44) (Fig. 5).

For the further analysis, the understanding of the dependencies of these elements from the supply chain network is important. These interactions are very complex and vary in among others intensity, frequency, or length (Goellner et al. 2010a, b, c).

The urgent need of a comprehensive categorization instrument like the "*Multi-layer Multiple Vector Model*" is the result of this complex situation.

Design and Development of a "State of the Art": Network Typology

For the generation of a final or semifinal product, there are a lot of various steps necessary. In Fig. 6, a possible supply chain is shown. The direction of the supply chain is not relevant at this moment.

Each circle stands for a company or organization independent of the organizational form. So, depending on the final product, a lot of different companies and organization work together in a more or less complex structure. The definition of clusters helps to reduce the complexity in a structured way (Buzan and Waever 2003, pp. 445–455). This is an important content for the relevance in development and operation of resilient supply chains (Christopher and Peck 2004, pp. 1–14; Fikar et al. 2015).

For the further analysis, it is important to assign the companies to defined main clusters. The main clusters are:

- acteur or trade cluster
- product cluster
- process cluster
- position cluster or areal cluster

The reason for the clustering based here on the consisting categorization systems like NACE or ÖNACE especially for Austria (WKO 2016 March 9). There are a lot of various additional systems like the following:

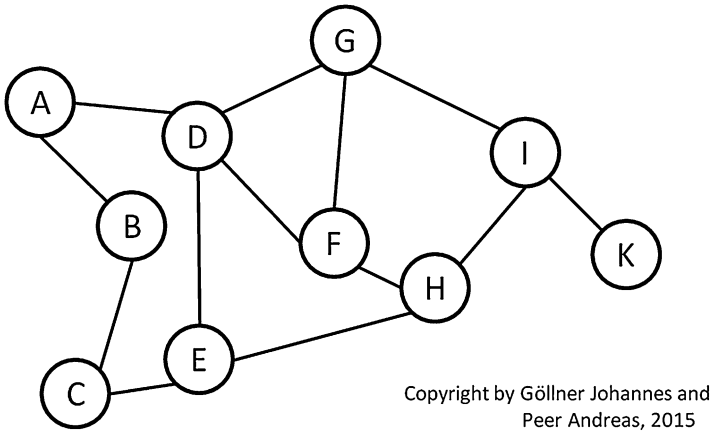


Fig. 6 Supply chain (Copyright by Göllner Johannes and Peer Andreas, 2015)

- ISIC is the United Nations' International standard industrial classification of all economic activities.
- HS is the harmonized commodity description and coding system, managed by the World Customs Organization.
- CPC is the United Nations' Central product classification.
- CPA is the European Classification of products by activity.
- PRODCOM is the classification of goods used for statistics on industrial production in the EU.
- CN stands for the combined nomenclature, a European classification of goods used for foreign trade statistics.

Such an integrated system allows the comparability of statistics produced in different statistical domains. As a consequence, for instance, statistics on the production of goods (reported in the EU according to PRODCOM surveys) could be compared with statistics on trade (in the EU produced according to CN) (Eurostat 2015).

For the further analysis of specific Supply chains, it may be purposeful to define additional clusters or subclusters on demand.

For each enterprise in the individual clusters, there are various defined key figures for the internal as well as for the external rating (Bornett et al. 2006, pp. 22–27). Exemplary for the intern rating of the bank sector defined by Basel II, which consists of hard and soft facts, there are among others following relative indicators relevant (Weber 2006, p. 48f; Howard 2009):

- equity ratio
- cash flow ratio
- return on sales

So, it is possible to compare the enterprises within the various clusters in a first step (Fig. 7).

In Fig. 6, the four basic clusters are visualized and in a second step the ranking within each cluster of the rating key figures may done with the individual rankings. Exemplary for the bank sector, there are following the NACE codes at least 24 different subclusters in the line of the acteur or trade cluster (Bornett et al. 2006, pp. 36–40). Next to the relevant rating key figures, the individual risk monitoring can be ranked within the individual cluster. So, it is possible to use the consisting individual risk rating and risk monitoring systems in the different clusters for the further analysis.

In the next step, the target-performance comparison for the cluster risk rating and risk monitoring system can be done with qualitative or quantitative methods.

Verification of the Relationships and Interfaces Along the Supply Chain Networks (SCN)

The Supply chain is defined as

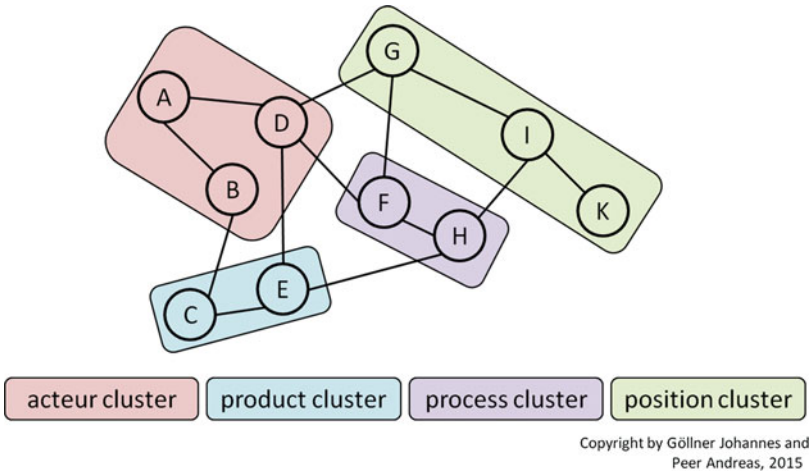


Fig. 7 Supply chain cluster (Copyright by Göllner Johannes and Peer Andreas, 2015)

> linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport. (ISO 28000 2007, p. 3)

So, the supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, and other entities that lead to the end user (ISO 28000 2007, p. 3).

On the other hand, there is the dependence of nearly every part of this supply chain from the various supply chain network. So, every so-called critical infrastructure or strategic infrastructure is part of the supply chain network. A general definition is not available but for this publication and the further understanding SCN is described as or consists of:

- natural physical networks and infrastructures
- manmade developed physical networks and infrastructures
- local, regional, national, international located or structured and centralized or decentralized located, structured, and operated
- all natural resources (e.g., air) and final or semifinal products or services

Further, consumer goods and capital goods and services are transported and provided by supply chain networks.

Mainly, the different critical or strategic infrastructures as part of the supply chain network are distinguished in:

- basic network and infrastructure
- supply network and infrastructure
- public administration network and infrastructure

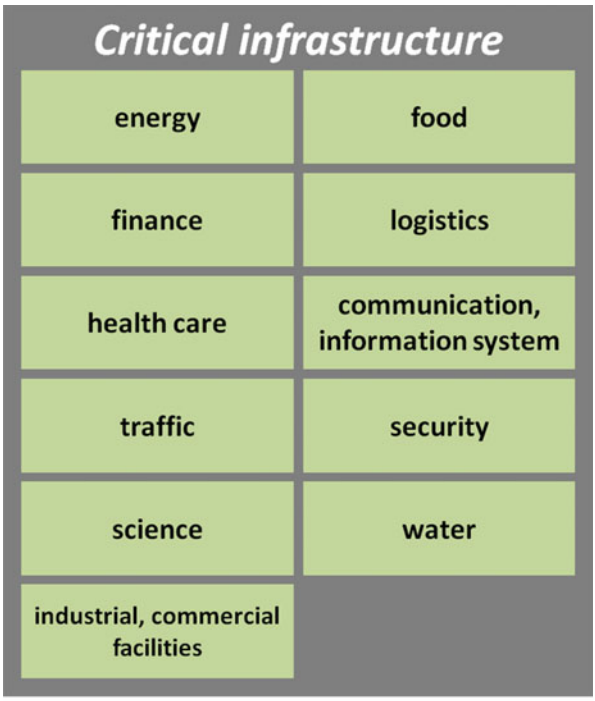


Fig. 8 Critical infrastructures (abstract) (Copyright by Göllner Johannes and Peer Andreas, 2011)

Some of these critical infrastructures (main layer) are visualized in Fig. 8.

The connection of the facilities, acteurs, etc. with the supply chain network depends of many various aspects like sort of acteur or location and is shown generically in Fig. 9.

There are a lot of various information and methods necessary to rank the individual interfaces with the elements of the supply chain network.

While the majority of laws and regulations relevant the implementation of an integrated supply chain risk, performance and security management (ISO 28001 2007, annex A-B) and monitoring system are based on European regulations, directives, and guidelines, US and Austrian national legislation and international and national standardizations and agreements (e.g., ISO 31000, ISO 31010, ISO 28000, ISO 28001, ON ISO 31000, ONR 49000ff) also play a major role.

For the monitoring of the relevant parts of the supply chain networks are a lot of individual or standardized semiautomatically or automatically systems available.

Due to the high degree of networking and dependency and innovation potential of the energy supply and the information and communication technology

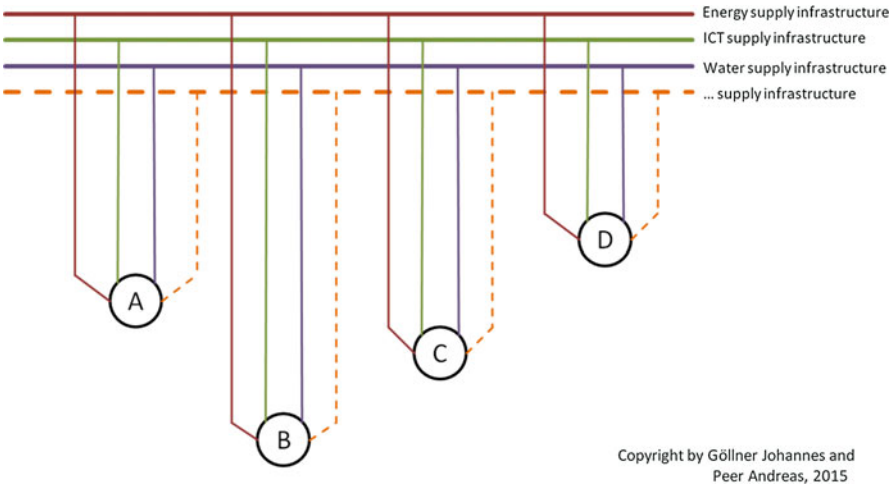


Fig. 9 Relationship of supply chain and supply chain network (Copyright by Göllner Johannes and Peer Andreas, 2015)

systems, there are a special field for research and development called Smart Grid.

The following infrastructures are part of the so-called Smart Grid:

- energy supply infrastructure
- ICT supply infrastructure

Smart Grids are defined in Austria as:

> A SmartGrid is an electricity network that can intelligently integrate the actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies. (E-Control 2016 June 25)

The European definition of Smart Grids are as follows:

> A Smart Grid is an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety. (European Commission 2011, p. 2)

Especially the smart grids are a rising topic with a huge risk potential especially for cyber threats. A policy framework and a minimum of security measures based on the existing standards and guidelines are still missing (enisa 2012 July 12). The involvement of various disciplines and stakeholders with different interests and often changing equipment is a challenge for the development of smart grids and especially under the aspect of the security of smart grids (Neureiter et al. 2016a, b).

Status Quo Monitoring and Rating

Rating models for the bank sector, for example, were implemented based on the Basel II reglementation. The rules must be applied according to the EU directives 2006/48/EC and 2006/49/since 1 January 2007 in the Member States of the European Union for all banks and financial services institutions.

The rating consists of the following components (Bornett et al. 2006, p. 14; Schmid and Untersperger 2012, p. 9):

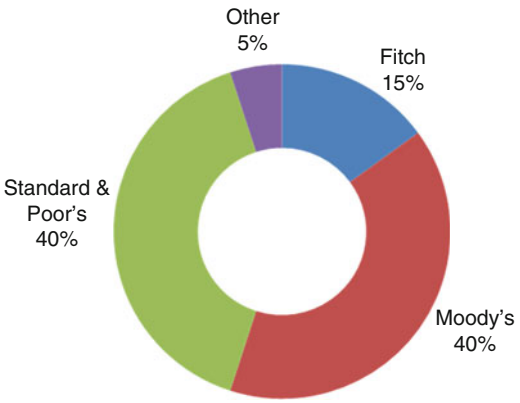
- hard facts or quantitative factors (e.g., balance sheet)
- soft facts or qualitative factors (e.g., managements skills)
- external and internal early warning indicators
- account data analysis (e.g., overdraft behavior)

Especially for the internal rating banks and financial services, institutions use the available hard facts. The ratings vary because of the individual ratings systems and weight factors.

In distinction to the internal rating, especially country risk, industry risk, and market risk as well as the operating policies of a company be considered in external rating by so-called rating agencies. The external ratings are generally available for all community of interests; on the other hand, the internal ratings are only available for the analyzed organization.

Also, the external ratings vary caused by the different methods and systems of the rating agencies. Unlike to the internal rating, there are only a few rating agencies for the complex and expensive external ratings (Fig. 10).

There are a lot of definitions for monitoring available because monitoring has a widespread application area. In general, monitoring is an umbrella term for all kinds of directly systematic recording, measurement, or observation, a process or



Source: Aithors' own visualization based on Handelsblatt 2011

Fig. 10 Rating agencies market sharing (Source: Authors own visualization based on Handelsblatt (2011))

procedure not only with technical means. An important function of monitoring is to interfere an ongoing process, for example, to maximize the output or reduce the losses.

There are a lot of various risk rating and risk monitoring systems implemented for specific requirements. For example, the Enterprise Value Map from Deloitte registers a huge amount of possible ways to improve shareholder values in a practical way as a kind of decision support. This is common way for decision makers to accelerate the connection between action they can take and shareholder value (Lukac and Frazier 2012, pp. 49–57).

Following the reference documents of the research, a comprehensive approach still does not exist and the available models fall too short and cannot capture the consisting complexity.

Generic Risk Monitoring and Risk Rating Model

Starting from the supply chain cluster, it is possible to compare the individual risk monitoring and risk rating systems. Overlaps and discrepancies can be identified easily and so the necessary nucleus for a generic risk rating system as well as for a generic risk monitoring system can be generated. The generic identification model is shown in Fig. 11.

Of course, this analyzation process must be done for all identified clusters of the whole supply chain applying the categorization logic like the "*Multi-layer Multiple Vector Model*."

Finally, the relevant parts of an integrated supply chain risk monitoring and supply chain risk rating system are identified as shown in Fig. 12. Therefore, the elements of

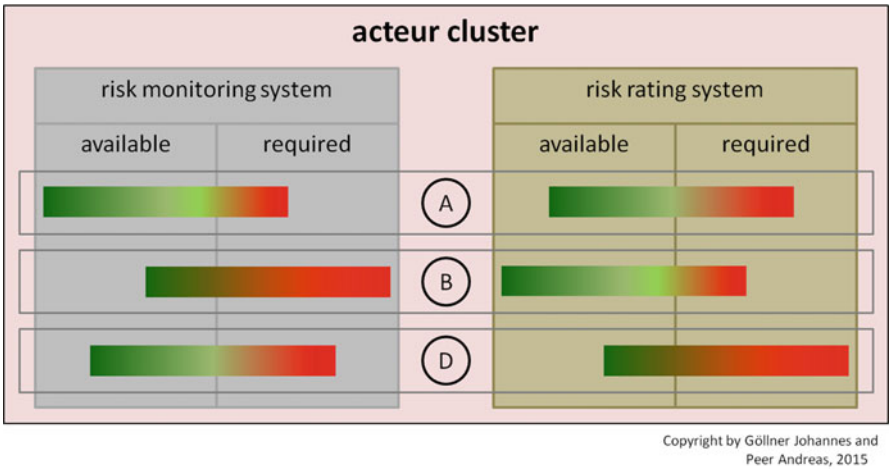


Fig. 11 Generic risk rating and risk monitoring identification model (Copyright by Göllner Johannes and Peer Andreas, 2015)

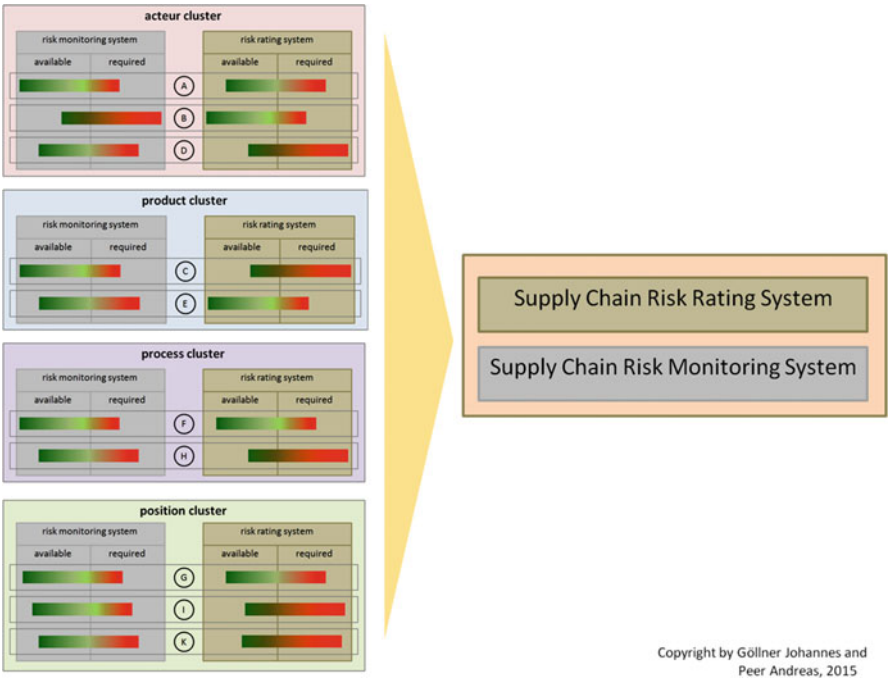


Fig. 12 Integrated supply chain risk rating and risk monitoring system (Copyright by Göllner Johannes and Peer Andreas, 2015)

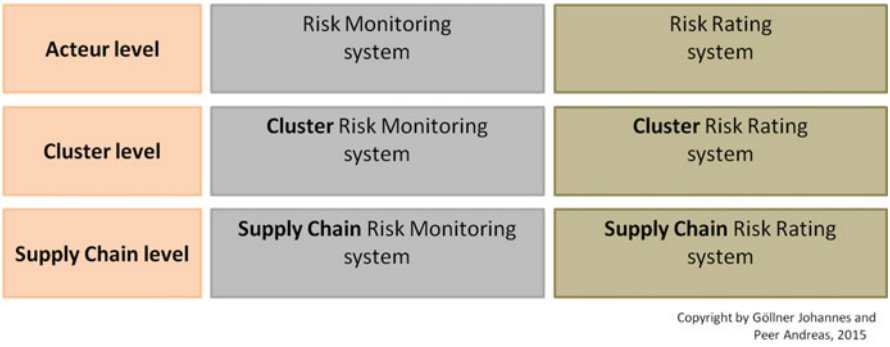


Fig. 13 Level-based rating and monitoring systems (Copyright by Göllner Johannes and Peer Andreas, 2015)

each individual identified cluster risk rating and risk monitoring systems must be combined together (Goellner and Peer 2012).

Based on the categorization logic from the "*Multi-layer Multiple Vector Model,"* there consist the following rating systems as shown in Fig. 13.

Due to the consistent application of the "*Multi-layer Multiple Vector Model,"* the red thread is running through all the levels. That allows the comparison within single clusters but also the comparison and ranking of some or all clusters of a supply chain under the aspect of the usability during all phases of the "*5-phase-model of Crisis Management*."

Risk Monitoring and Risk Rating Model for Supply Chain Networks

So far, the process has been performed bottom-up. The concentration was primarily on the consistent orientation along the "*Multi-layer Multiple Vector Model*." Now takes place the reversal of the approach. Based on the strategic level rating, the influences of the single critical infrastructures are able to be identified easily for various issues.

So, the risk management process is implemented for the single acteurs up to the identified clusters and after all for the total supply chain.

Another important point of view is the identification and of course rating and monitoring of the influence from a part of the supply chain network on parts of the supply chain and overall also on other parts of the supply chain network.

The focus of the single and modular rating and monitoring systems is, following the "*5-phases-model for Crisis Management*," the reduction of

- the disaster intensity
- execution and follow-up phase

which are shown in Figs. 14 and 15 (KIRAS 2013b, pp. 24–27).

So, the necessary resources can be used in an efficient and effective way for the disaster management and of course for the business continuity management.

The integrated application of this intermeshing operational and strategic models allows the identification of the relevant scenarios, risk rating, and key performance factors for the considered hierarchical layer. So, the development of an integrated supply chain risk monitoring and risk rating system is possible and necessary as well as the corresponding rating and monitoring systems for the various operational layers.

Conclusion

The need of an integrated risk monitoring and risk rating system for supply chain networks continuously increase as well as the use of the operational risk monitoring and risk rating systems.

The intermeshing of different specific and individual systems is mandatory for an efficient and effective risk management as well as disaster management or business continuity management.

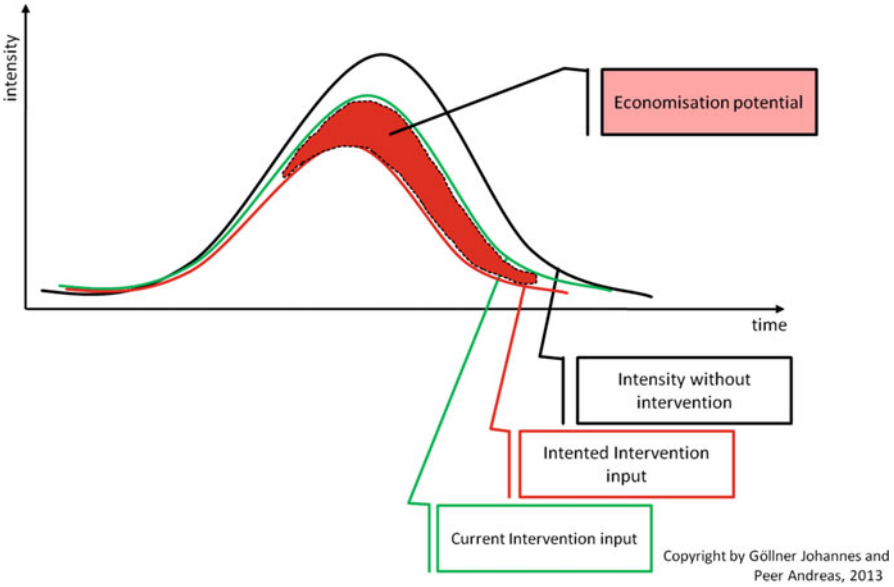


Fig. 14 Economic potential – intensity (Copyright by Göllner Johannes and Peer Andreas, 2013)

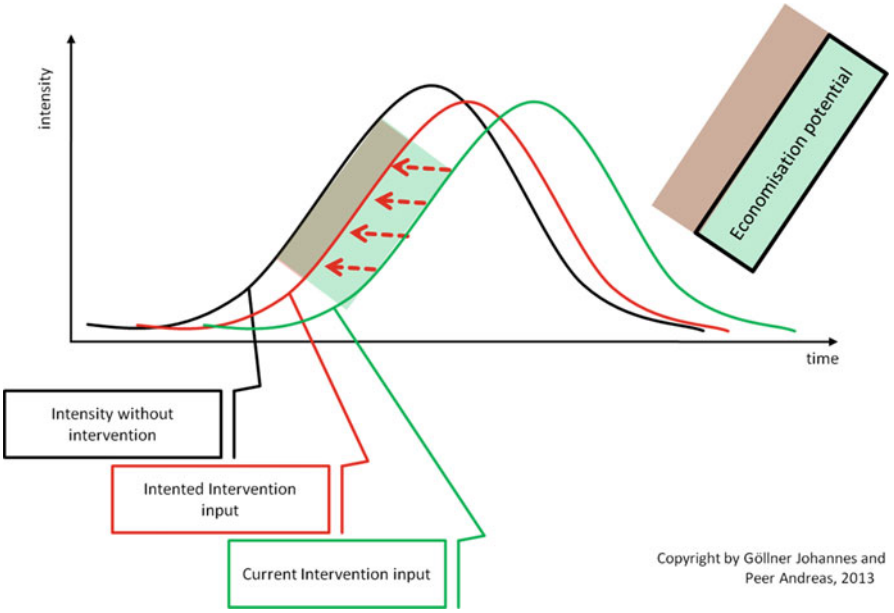


Fig. 15 Economic potential – time (Copyright by Göllner Johannes and Peer Andreas, 2013)

Of course, there are some possibilities to use parts of the consisting and implemented systems but always under the aspect of a standardized categorization model like the "*Multi-layer Multiple Vector Model.*"

The development of such a supply chain network risk rating and risk monitoring system is the basis for the further development of existing real-time decision support system, concepts, models, methods, and tools as part of corporate information systems.

With such an integrated supply chain risk monitoring and supply chain risk rating model also future trend analysis and foresight analysis are possible, either specific or in general.

With a supply chain network risk rating system and supply chain risk monitoring system, decision makers on the strategic level are able to use readily available and consistent information based on structured complex concerted analysis for their strategic decision-making process.

Especially in complex and rapidly changing areas like Smart Grid up to Smart Economies but also the aspect of the resource security (e.g., raw materials) taking account the circumstances of among others of the cyber security such an integrated supply chain risk rating and supply chain risk monitoring system is essential. The complexity of the supply chain networks (abstract) and the increasing topic of Smart Grids up to Smart Economy is visualized in Fig. 16.

Of course, this logic model can find application to all other topics.

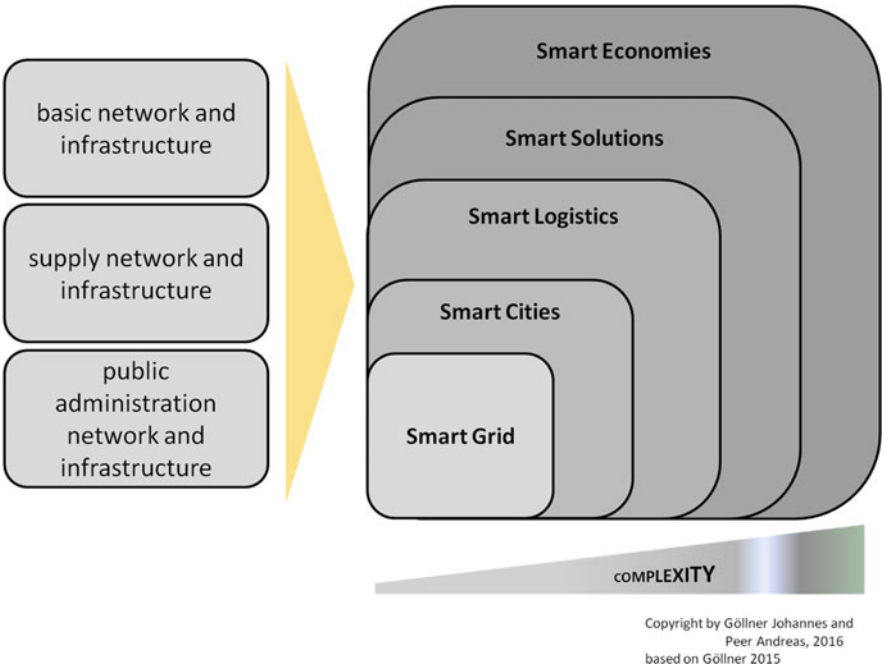


Fig. 16 Interdependencies and complexity of smart development (Copyright by Göllner Johannes and Peer Andreas 2016 based on Göllner 2015)

Cross-References

- ▶ Citizenship Education and New Media: Opportunities and Challenges
- ▶ Concept for Strategic Foresight Knowledge Development Framework for Horizon Scanning Center
- ▶ Crowdsourcing Social Innovation: Toward a Collaborative Social Capitalism
- ▶ Cyber-Democracy and Cyber-Defense
- ▶ Cyber Documentation and Research Center "Horizon Scanning Center" for Cyber Analysis and Monitoring
- ▶ Cyber Insurance
- ▶ Knowledge Society, Knowledge Economy, and Knowledge Democracy
- ▶ Mining Governance Mechanisms: Innovation Policy, Practice, and Theory Facing Algorithmic Decision-Making
- ▶ Media in Knowledge Democracy and Cyber-Democracy
- ▶ Society in Need of Future: Complementary Foresight as a Method to Co-create Transition
- ▶ The Role of Information and Communication Technology (ICT) in the Governance of Energy Access: Exploring Application of Quadruple and Quintuple Helix Innovation Theory in Technology Transfer
- ▶ Welfare in a Competitive European Union? Some Aspects of Cybernetic Higher Education (HE) Policy in Knowledge Generation

References

Backfried, G., Göllner, J., Quirchmayr, G., Rainer, K., Kienast, G., Thallinger, G., Schmidt, C., & Peer, A. (2013). Integration of media sources for situation analysis in the different phases of disaster management. In *EISIC 2013-European intelligence and security informatics conference, August 12–14, Uppsala, Sweden*.

Backfried, G., Schmidt, Ch., Aniola, D., Meurers, Ch., Mak, K., Göllner, J., Peer, A., Quirchmayr, G., Czech, G., & Glanzer, M. (2016). A general framework for using social and traditional media during natural disasters: QuOIMA and the Central European Floods of 2013, Chapter 22. In *Fusion methodologies in crisis management higher level fusion and decision making*. Springer, Cham.

BKK. (2011). Sony postpones product launches due to Thailand floods. Retrieved from http://www.bbc.co.uk/news/business-15380718. Accessed 22 May 2014.

Bornett, W., Bruckner, B., Hammerschmied, H., & Masopust, H. (2006). *Rating-Kennzahlen 24 Branchen im Vergleich*. WKO Abteilung für Finanz- und Handelspolitik, Vienna.

Buzan, B., & Waever, O. (2003). *Regions and powers. The structure of international security* (6th ed.). Cambridge University Press. ISBN 978-0-521-81412-6.

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security – A new framework for analysis*. Lynne Rienner Publications, Colorado. ISBN-13: 978-1555877842.

CCN-CERT. (2016). *CCN-CERT IA-09/16, cyber threats 2015/trends 2016* [Executive summary].

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management, 15*(2), 1.

Controller Magazin. (2016). Allianz Risk Barometer 2016: Die Top-10 der größten Geschäftsrisiken 2016, Ausgabe 3, 2016, München.

Cross-border Research Association. (2012). Problem space report: Critical infrastructure & supply chain protection; Deliverable 5.1; FP 7 – SEC – 2010 – 1, Foresight security scenarios – Mapping research to a comprehensive approach to exogenous EU roles.

Deutsche Post AG. (2012). *Delivering tomorrow – Logistic 2015 – A scenario study*. Deutsche Post AG, Bonn.

E-Control. (2016 June 25). Smart grids. Retrieved from https://www.e-control.at/marktteilnehmer/strom/fachthemen/smart-grids#

enisa. (2012 July 12). New ENISA study: 10 recommendations for making European smart grids safer, Press release. European Union Agency for Network and Information Security. Retrieved from https://www.enisa.europa.eu/news/enisa-news/new-enisa-study-10-recommendations-for-making-european-smart-grids-safer

European Commission. (2011). Definition, expected services, functionalities and benefits of smart grids, COM(2011) 202 final, Brussels 2001.

Eurostat. (2015 March 23). NACE background. Retrieved from http://ec.europa.eu/eurostat/statistics-explained/index.php/NACE_background

Fikar, Ch., Gronalt, M., Goellner, J., & Hirsch, P. (2015). Simulation-optimisation based decision-support for coordinated disaster relief last-mile distribution. Presented at the I3M 2015 – the 12th International Multidisciplinary Modeling & Simulation Multiconference from 21–23 Sept 2015 in Bergeggi.

Goellner, J. (2015). *Smart economies/smart solutions-finance, science cloud alligned by Center for Risk and Crisis Management*, 2015 Oct, Vienna.

Goellner, J., & Peer, A. (2012). Modelling of an risk rating model for analysis and auditing of strategic supply chain networks. Presentation at the 5th standardization-workshop for "supply chain risk management" of the Risk Management Association at the Munich Re, 20 Sept 2012, Munich.

Goellner, J., Meurers, C., Peer, A., & Povoden, G. (2010a). Wissensmanagement im ÖBH (Knowledge Management in the Austrian Armed Forces). Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und Modellierung (Definition, description and boundary of systems). Teil 1: Allgemeine Systemdefinition und Systembeschreibung (Part I: General definition and description of systems). Schriftenreihe der Landesverteidigungsakademie, 12/2010. Reprozentrum Wien 4450/10. ISBN: 978-3-902670-51-9.

Goellner, J., Meurers, C., Peer, A., & Povoden, G. (2010b). Wissensmanagement im ÖBH (Knowledge Management in the Austrian Armed Forces). Systemdefinition, -beschreibung und –begrenzung zur Szenarioentwicklung und Modellierung (Definition, description and boundary of systems). Teil 2: Darstellung von ausgewählten Methoden und möglichen Teilsystemen (Part II: Description of selected methods and possible subsystems). Schriftenreihe der Landesverteidigungsakademie, 13/2010. Reprozentrum Wien 4684/10. ISBN: 978-3-902670-53-3.

Goellner, J., Meurers, C., Peer, A., & Povoden, G. (2010c). Einführung in die Soziale Netzwerkanalyse und exemplarische Anwendungen (Introduction of Social Network Analysis and selected applications). Wissensmanagement im ÖBH (Knowledge Management in the Austrian Armed Forces). Schriftenreihe der Landesverteidigungs-akademie, 5/2010/S. Reprozentrum Wien. ISBN 978-3-902670-56-4.

Goellner, J., Kienesberger, G., Peer, A., Schoenbacher, P., Weiler, M., & Wurzer, G. (2010d). Analyse und Betrachtung von Kritischen Infrastrukturen (Analysis and description of critical infrastructures). Schriftenreihe der Landesverteidigungsakademie, 14/2010/S. Reprozentrum Wien 4889/10. ISBN: 978-3-902670-64-9.

Goellner, J., Meurers, C., Peer, A., & Povoden, G. (2011). Hybridisation of social network analysis in context with other methods for a scenario based risk analysis-case study: Critical infrastructure for energy security in Austria. In *7th social network conference 2011 at the University of Greenwich, London, United Kingdom*.

Goellner, J., Meurers, C., Peer, A., Langer, L., & Kammerstetter, M. (2014a). Bedeutung des Risikomanagements für die Sicherheit von Smart Grids (relevanz of risk management for security of smart grids). In *Proceeding of the 13. Symposium Energieinnovation EnInno 2014*, Graz.

Goellner, J., Peer, A., Gronalt, M., & Quirchmayr, G. (2014b). Risk analysis for supply chain networks. Presented at the I3M 2015 – the 11th International Multidisciplinary Modeling & Simulation Multiconference in Sept 2014, Bordeaux.

Handelsblatt. (2011 July 18). Die mächtigen Ratingagenturen im Überblick. Retrieved from http://www.handelsblatt.com/unternehmen/handel-konsumgueter/sundp-moodys-fitch-und-co-die-maechtigen-ratingagenturen-im-ueberblick/4404776.html

Howard, P. (2009). *Research into the definition and application of the concept of risk appetite*. University of Nottingham, Nottingham.

ISO 28000. (2007). *International standard – Specification for security management systems for the supply chain*. Geneva: International Organisation for Standardization.

ISO 28001. (2007). *International standard – Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance*. Geneva: International Organisation for Standardization.

KIRAS. (2013a). MetaRisk Meta-Risiko-Modell für kritische Infrastrukturen, Kooperative F&E-Projekte, Projektantrag.

KIRAS. (2013b). LMK-MUSE Modellbildungs- und simulationsgestützte Entscheidungsunterstützung in der Last-Mile Katastrophenbewältigung, F&E-Projekte, Projektantrag.

Liebig, M. (2010). *Reaktivierungsmanagement von Not leidenden Unternehmen, Sanierungsmöglichkeiten im Rahmen der Insolvenzordnung*. Gabler Verlag.

Lukac, E. G., & Frazier, D. (2012). Linking strategy to value. *Journal of Business Strategy, 33*, 49.

modulushca. (2016 June 25). MODULUSHCA – Modular logistics units in shared co-modal networks. Retrieved from http://www.modulushca.eu/

Neureiter, Ch., Uslar, M., Engel, D., & Lastro, G. (2016a). A standards-based approach for domain specific modelling of smart grid system architectures. System of Systems Engineering Conference (SoSE). 2016 June 11th in Kongsberg, Norway and to IEEE Xplore at 15 August 2016.

Neureiter, C., Engel, D., & Uslar, M. (2016b). Domain specific and model based systems engineering in the smart grid as prerequesite for security by design. *Electronics, 5*, 24.

North Atlantic Treaty Organization. (2013). *Strategic foresight analysis 2013 report*. Retrieved from http://www.sicherheitsforschung-europa.de/servlet/is/17284/Strategic%20Foresight%20Analysis%20%20FINAL_PRINTABLE.pdf?command=downloadContent&filename=Strategic%20Foresight%20Analysis%20%20FINAL_PRINTABLE.pdf

North Atlantic Treaty Organization. (2015). *Strategic foresight analysis workshop-Helsinki*, Helsinki, 21–22 Oct 2015. Retrieved from http://www.act.nato.int/images/stories/events/2012/fc_ipr/sfa201701-4.pdf

Peer, A. (2004). Analyse und Betrachtung von Systemen zur Dekontamination von Großgerät nach militärischen ABC-Einsätzen und/oder zivilen ROTA-Ereignissen, Diplomarbeit, Wr. Neustadt, Mai 2004.

Peer, A., Göllner, H., Haberfellner, C., & Bauer, H. (2014a). Risk analysis for "Schutz 14". European meetings on cybernetics and systems research 2014 – Session risks in supply chain networks. Civilisation at the Crossroads Response and Responsibility of the Systems Sciences, Book of Abstracts, pp. 628–632, Vienna.

Peer, A., Fikar, Ch., Hirsch, P., Goellner, J., Gronalt, M., & Quirchmayr, G. (2014b). Modelling simulation-based decision support in the last mile of crisis management. Presented on the European Meetings on Cybernetics and Systems Research (EMCSR) 2014 from 22–25 Apr 2014 in Vienna.

Plattform Industrie 4.0. (2015). Umsetzungsstrategie Industrie 4.0, April 2015.

Poustourli, A., & Kourti, N. (2014). Standards for Critical Infrastructure Protection (CIP) – The Contribution of ERNCIP.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems*. Magazine, pp. 11–25

Risk Management Association e.v. (2015). Leitfaden für das Supply Chain Risk Management – Schaffung einer einheitlichen Basis für das unternehmensübergreifende Management von Supply Chain Risiken, 2015.

Schmid, Ch., & Untersperger, A. (2012). *Ratingagenturen Verursacher oder Sündenböcke der Wirtschaftskrise?* WKO Abteilung für Finanz- und Handelspolitik, Vienna.

TU Graz. (2016 July 02). Die Ultrahochleistungsfahrbahn im ersten Stock. Retrieved from https://www.tugraz.at/tu-graz/services/news-stories/planet-research/einzelansicht/article/die-ultrahochleistungsfahrbahn-im-ersten-stock/

Vester, F. (2008). *Die Kunst vernetzt zu denken. Ideen und Werkzeuge für einen neuen Umgang mit Komplexität* (7th ed.). München: Deutscher Taschenbuch Verlag.

Weber, M. (2006). *Schnelleinstieg Kennzahlen*. München: Rudolf Haufe Verlag GmbH & Co. KG.

Wilding, R. (2011 May 22). Supply chain resilience & supply chain strategy: A story of the unexpected. Cranfield University School of Management, lecture presentation. Retrieved from http://www.bring.no/load/foredragsholdere/foredragsholdere-2012/_attachment/308935?_download=true&_ts=139f9b3dd30

WKO. (2016 March 9). ÖNACE 2008 – Klassifikation der Wirtschaftstätigkeiten. Retrieved from https://www.wko.at/Content.Node/Interessenvertretung/ZahlenDatenFakten/Oenace_2008_2014.html

Cyberwar and Cyberpeace

42

Stefan Hügel, Hans-Jörg Kreowski, and Dietrich Meyer-Ebrecht

Contents

S. Hügel (✉)
Forum Computer Professionals for Peace and Social Responsibility (FIfF), Bremen, Germany
e-mail: sh@fiff.de

H.-J. Kreowski
Computer Science Department, University of Bremen, Bremen, Germany
e-mail: kreo@informatik.uni-bremen.de

D. Meyer-Ebrecht
RWTH Aachen, Institute of Imaging and Computer Vision, Aachen, Germany
e-mail: dme@fiff.de

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_41

Abstract

For a decade at least, a worldwide cyber armament race takes place; cyber attacks against all kinds of information and communication systems are a daily reality, and cyberwar becomes a growing threat. In this chapter, the military, political, and technological aspects of cyberwar are surveyed and discussed on one hand. On the other hand, the vision of cyberpeace is sketched as a counter-concept.

Keywords

Cyber security · Cyber weapons · Cyberpeace · Cyberwar · International law · Internet · Military · Surveillance

Introduction

In the beginning of their development, the Internet and all telecommunication infrastructures – commonly referred to as *Cyberspace* – seemed to be a great promise. Worldwide communication was expected to be the basis of international understanding and peace.

Today, however, one must acknowledge that the Internet has never got out of the focus of the military, being used as an instrument to prepare for cyberwar and worldwide communication surveillance resulting in a far-reaching military colonization of the Internet. More than 100 states worldwide have enacted cyberwar strategies that endanger civil society and civil infrastructure. The cyberwar policies of these states reach from the total surveillance of digital communication through a spectrum of means and forms of espionage and sabotage to the massive armament based on information technology. In this chapter, the political, military and technological circumstances of the growing threats of cyber attacks are surveyed and discussed.

Moreover, the idea of cyberpeace as a counter-concept to cyber warfare is elaborated. It includes the prohibition of cyber attacks in the Internet and by means of other information technologies. The military colonization of the Internet is rejected – the goal is an Internet that serves international understanding, worldwide peace and well-being of humankind.

In more detail, the chapter is divided in three parts. The first one concerns the military and political aspects of cyberwar including a discussion of the notion, of cyberwar units, of cyber attacks, of the endangerment of the civil society and of the secret-service surveillance. Moreover, cyberwar is considered with respect to cyber strategies, the political and military attraction, the risk of war, and the international

laws of war. The second part focuses on the technological aspects. Starting with some security basics, the vulnerability of information and communication systems, the tools of cyber attacks, and their effects are discussed. The part ends with a consideration of countermeasures. The third part outlines the framework of cyberpeace that covers four issues: rebuilding trust, resolving conflicts in a non-violent way, securing vital infrastructures, and preserving democratic political control.

The chapter is based in parts on the papers (Johnigk et al. 2014; Hügel 2016) as well as on an unpublished manuscript by the third author.

The Military and Political Aspects of Cyberwar

The Notion of Cyberwar Is Hard to Determine

Cyberwar is an iridescent term that refers to all kinds of military attacks on the information and communication infrastructure of states by means of information and communication technology (ICT). Not all cyber attacks should be subsumed under the umbrella of cyberwar, although the techniques and methods they employ are often similar. There is quite a lot of cyber fraud, online theft, phishing, and the like that can be addressed as cyber crime. There are forms of online protest as politically motivated actions – also referred to as *hacktivism* – that should not be mixed up with military operations. Cyber espionage is often economically or politically motivated rather than by military purposes. Even cyber sabotage and cyber terrorism are not automatically military affairs. Cyberwar activities are not easily separated from criminal and terroristic cyber attacks in any case, but they should not be confused with them.

Some experts argue that cyberwar is a misleading and wrong term and that the phenomenon is more properly called terrorism, espionage, and sabotage (cf., e.g., Rid 2012). But others take the term quite seriously, like the authors of a spectrum of nonfiction books (Brenner 2009; Stiennon 2010; Gaycken 2011; Ventre 2011; Carr 2012; Clarke and Knake 2012; Costigan and Perry 2012; Gaycken 2012; Singer and Friedman 2014; Stiennon 2015; Ventre 2016 and others).

Cyberwar Units

Cyberwar is not a chimera, but a real danger. Evidence is the fact that more than 100 states in the world have built up cyberwar units. Among them one finds the following:

USA: The US Cyber Command (USCYBERCOM) was initiated as a sub-command of the US Strategic Command in 2009. According to the webpage https://www.stratcom.mil/factsheets/2/cyber-command, its mission is: "*USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and* defense *of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable*

actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries." In addition, there is the National Security Agency (NSA) that is described on its webpage https://www.nsa.gov by: "*The National Security Agency/Central Security Service (NSA/CSS) is a key member of the Intelligence Community and, by its very nature, requires a high degree of confidentiality. The Agency collects, processes, and disseminates intelligence information from foreign electronic signals for national foreign intelligence and counterintelligence purposes and to support military operations. NSA/CSS is also tasked with preventing foreign adversaries from gaining access to classified national security information."* And in another section, it says: "*The National Security Agency is part of the U.S. Department of Defense, serving as a combat support agency. Supporting our military service members around the world is one of the most important things that we do."*

United Kingdom: The Government Communication Headquarters (GCHQ) is in charge of the national cyber security in the United Kingdom. On the webpage https://www.gchq.gov.uk in the section *What we do*, the aim is formulated: *"Using our expertise and experience GCHQ is part of the team which protects the UK, along with law enforcement and the* other *intelligence agencies. Working with HMG* (i.e. Her Majesty's Government, the authors) *and industry, we defend Government systems from cyber threat, provide support to the Armed Forces and strive to keep the public safe, in real life and online."* In the section *Cyber security* one can read more specifically: *"CESG, the Information Security arm of GCHQ, protects the vital interests of the UK by providing advice on Information Assurance Architecture and cyber security to UK government, critical national infrastructure, the wider public sector and suppliers to UK government."*

France: The Network and Information Security Agency (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI) was set up in 2009. It is the French national authority for the security of information systems attached to the Secretary General of Defense and National Security (SGDSN), who reports to the Prime Minister. On the webpage http://www.ssi.gouv.fr in the section *Cyber security in France*, one can read: "*ANSSI was created in line with the proposals of this White Paper on Defense and National* Security. *A strategic committee for cybersecurity was set up by ANSSI's founding decree in order to propose a national cybersecurity strategy."*

Germany: The German government reacted to the growing threat by cyber attacks and the worldwide cyber armament later than most other leading countries. In 2011 and 2012, the National Cyber Security Council (*Nationaler Cybersicherheitsrat*), the National Cyber Defense Center (*Nationales Cyberabwehrzentrum*), and the Alliance for Cyber Security (*Allianz für Cybersicherheit*) were constituted. The first two organize the cooperation of security-related ministries and other governmental security institutions including police, secret service, and the German armed forces. The latter serves for the coordination and consultation between the Federal Office for Information Security (*Bundesamt für die Sicherheit in der Informationstechnik, BSI*) and the major players in ICT. In this year, the Minister of Defense, Ursula von der Leyen announced the formation of a new

cyberwar unit within the German armed forces. Its official name is *Organization Unit Cyber and Information Space* (*Organisationseinheit Cyber- und Informationsraum, CIR*), and it will consist of about 14,000 military and civil posts. Its mission is mainly described by the terms cyber defense and cyber security. But there are also clear hints that the unit will be in charge of the development and deployment of offensive cyber weapons. More details – unfortunately only in German – can be found in a report of a task force on cyber and information space (Federal Ministry of Defense 2016).

Israel: A Cyber Defense Taskforce was constituted. The Jerusalem Post (http://www.jpost.com/Breaking-News/PM-announces-new-cyber-defense-taskforce) distributed the following note on May 18, 2011: *"The Prime Minister's Office has announced the establishment* of *a taskforce to encourage and develop Israel's defense capabilities against cyber terrorism, said a statement published on the PMO's Facebook page Wednesday. The taskforce is also expected to help turn Israel into a source for global knowledge on cyber defense, in cooperation with members of academia, the defense industry, and other public bodies."*

Iran: The Iranian Cyber Army, which may be closely related to The Islamic Revolution Guards Corps, is assumed to be very active with respect to cyber attacks. Moreover, there are more official organizations in operation. In an article of the L'Institut Français d'Analyse Stratégique (IFAS) (http://www.strato-analyse.org/fr/spip.php?article223#outil_sommaire_3), one finds the following statement: *"In Iran, the highest government body that deals with the cyberspace is a newly-established organization named the High Council of Cyberspace (Shoray-e Aali-e Fazaye Majazi). In March of 2012 this new structure was set up on the orders of Ayatollah Khamenei with the mission of instituting high-level policies on the cyber-space. After the foundation of the High Council of Cyberspace, all other Iranian organizations in charge of cyber operations are committed to implement the policies instituted by this new government body."*

China: The country is suspected to run a spectrum of organizations in charge of cyber defense, cyber attack, and espionage including the General Staff Department, Third and Fourth Departments, several Technical Reconnaissance Bureaus as well as People's Liberation Army (PLA) Information Warfare Militia Units. While always denied earlier, one could find on the website http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html recently: *"A high-level Chinese military organization has for the first time formally acknowledged that the* country's *military and its intelligence community have specialized units for waging war on computer networks. China's hacking exploits, particularly those aimed at stealing trade secrets from U.S. companies, have been well known for years, and a source of constant tension between Washington and Beijing. But Chinese officials have routinely dismissed allegations that they spy on American corporations or have the ability to damage critical infrastructure, such as electrical power grids and gas pipelines, via cyber attacks."*

Russia: Similarly, it is believed that both the Federal Security Service (FSB) and the Ministry of Defense are the leading agencies for cyberwar activities in Russia. The SFB is described on the official webpage (http://government.ru/en/department/113/) as follows: *"The Federal Security Service (FSB) is a federal executive body*

with the authority to implement government policy in the national security of the Russian Federation, counterterrorism, the protection and defense of the state border of the Russian Federation, the protection of internal sea waters, the territorial sea, the exclusive economic zone, the continental shelf and their natural resources, ensuring the information security of Russia and exercising the basic functions of the federal security services specified in the Russian legislation, as well as coordinating the counterintelligence efforts of the federal executive bodies that have the power to do so."

The list of cyberwar units compiles some important examples but is far from being exhaustive. While the mission of cyberwar units all over the world addresses mainly cyber security and defending against cyber attacks, the development and use of offensive cyber weapons are also in the focus in most of these organizations. It is interesting to note that not only the topic of cyber security is often merging civil and military security, but that also the offensive cyber capabilities are a domain of the intelligence agencies such as the National Security Agency (NSA) in the United States and GCHQ in the United Kingdom.

The Reality of Cyber Attacks

During the last decade and longer, a long list of severe incidents has been encountered that can be addressed as cyber attacks. Typical examples are the following:

- Much public attention got the operation *Titan Rain*, a series of coordinated cyber attacks against the US Forces, the NASA, armaments groups, and others running from 2003 for about 3 years. It is generally assumed that the attacks were implemented by Chinese hackers, but a confirmed attribution is missing (confer https://en.wikipedia.org/wiki/Titan_Rain).
- The operation *Olympic Games* with the computer worm Stuxnet became particularly famous. The malware was developed in various versions since about 2005 in cooperation between the United States and Israel. It had quite a damaging effect in 2010 on Iranian uranium enrichment facilities, the intended target. But other countries were also affected (confer https://en.wikipedia.org/wiki/Stuxnet). While most known malware steals information or denies web services or disrupts computer systems, Stuxnet is considered to be one of the first cyber weapons that can cause physical destruction of computer-controlled machinery.
- Among the many denial-of-service attacks against companies of various kinds, bank institutes, public media, and governmental institutions, one has encountered quite severe attacks disrupting the Estonian and the Georgian websites in 2007 and 2008, respectively. In both cases, Russia was suspected as origin.
- In May 2015, a drastic cyber attack on the German parliament was uncovered. The used malicious software infected more than 20.000 accounts of the parliament network. The damage amounts to millions of Euros. Russian intelligence agencies have been blamed for the attack.

The list could be prolonged by an unbelievably large number of incidents. In many cases, it is not proved where the attacks came from or who launched them. The attribution of cyber attacks is a big problem. Often, it is also not so clear which aims the attacks have. Espionage and sabotage play a role, but attacks may also be meant as provocation, warning, revenge, or just as training of hacker groups.

Cyberwar Endangers the Civil Society

As the examples above indicate, means of cyber warfare pose potential threats on nations and societies, which are summarized under four categories:

- Threats to civil rights, such as freedom and privacy, through means of secret service surveillance
- Threats to life and corporal integrity of humans through cyberwar attacks leading to real-world effects, for example, drone attacks against humans – remotely or autonomously controlled via data networks and computer systems
- Threats to technical equipment via malicious software, for example, the Stuxnet worm attacking an Iranian uranium enrichment plant in 2010 (see above).
- Threats to democracy and civil society, through manipulation and misleading public opinion by publishing falsified or "biased" information

These threats must be taken seriously and appropriate measures must be taken to prevent society from their dangerous effects. To elaborate the threats of cyberwar, the issue of surveillance is discussed in more detail.

Secret Service Surveillance

Anonymous communication without surveillance is a fundamental right; privacy of correspondence and telecommunication is guaranteed by constitution in democratically constituted nations (in Germany, for example, by article 10 of the German constitutional law (Federal Ministry for Justice and Consumer Protection 2012)). Not only since the disclosure of US intelligence documents by Edward Snowden, however, one must state, that communication without surveillance has been only an illusion in most parts of the world. The most widely known measure of surveillance was probably the *Echelon* system to intercept satellite communication, among others performed on the US base in Bad Aibling in Bavaria. Although criticism emerged when Echelon became known to the public, this criticism subsided quickly after the terrorist attacks of September 11, 2001, the beginning "War on Terror" and following legislation like the PATRIOT Act in the USA. Nevertheless, the reports on Echelon already have shown the intention (not only) of American authorities to establish and continue mass surveillance – regardless of constitutional restrictions.

In Germany, the historian Josef Foschepoth from the University of Freiburg published a study in 2012, which showed that not only in the German Democratic

Republic, but also in the Federal Republic of Germany communication had been intercepted since the end of the Second World War – during the Cold War and after the reunification of the German states in 1990 (Foschepoth 2012). In the beginning, this was legally justified by occupational law. Later, in 1968, privacy of communication was restricted by the G10 act ("G10" referring to article 10 of the constitutional law), which, in addition, suspends legal remedy if human rights are violated by surveillance measures (Federal Ministry for Justice and Consumer Protection 2001). Instead of providing this basic right, which is a crucial element of civil rights in a constitutional state, a parliamentary commission (G10-Commission) was established and assigned the task of reviewing the legality of surveillance measures under the G10 act. It must be doubted that these reviews can be effective, regarding the commission's limited capacity.

The amount of documents disclosed by Edward Snowden in 2013, however, exceeded the amount of information on governmental surveillance publicly available before by far (Greenwald 2014). The disclosure made clear the extent and the worldwide nature of the surveillance programs by intelligence agencies from the USA and in other nations, including EU members Great Britain, France, Germany, and others. For interception, vulnerabilities of the communication systems are required to be exploited through malicious software. Vulnerabilities for interception may be achieved in two ways

- by exploiting existing vulnerabilities
- by creating new vulnerabilities

Either way, preparing for surveillance often is the beginning of cyberwar and compromises the communication infrastructures our society and our economy relies on – any attacker might use the vulnerabilities which have either not been disclosed or have been actively created to attack vital computer systems and infrastructures. Exploiting existing vulnerabilities requires not to disclose known vulnerabilities of the systems and so not to repair them. Creating new vulnerabilities means to actively attack the systems – this already might be understood as an act of cyberwar.

When the information on worldwide surveillance was disclosed by Edward Snowden in 2013 (Greenwald 2014), expectations were raised that secret service surveillance in the massive extension observed would lead to civil protests and, as a further development, to the reduction of surveillance, restoration of civil rights in cyberspace, and in general. Instead, among others justified by terrorist attacks in the United States, France and Belgium, surveillance still proceeds and has even been extended in recent years. So, as surveillance and its surrounding framework persist, also the danger to freedom and civil rights associated with it continues. We, as members of a free society, must determine the red line, where freedom and civil rights are in jeopardy, and the range, where we want to accept surveillance and restrictions of civil rights in order to achieve an asserted grade of security.

Cyber Warfare and Cyber Strategies

Besides the endangerment of the civil society, networked communication infrastructures are the basis for cyberwar in its original sense. It may be used by military to conduct wars and harm perceived enemies, e.g. by introducing malicious software into their computer systems. Also drone attacks, killing humans who are considered "terrorists" (and their bystanders), in most cases without legal consideration, use these communication infrastructures – directed from the United States and, for instance, mediated via Ramstein, a military base operated by the USA in Germany (Scahill 2015). So the Internet today serves as a basic technology for military action: It is under surveillance by intelligence services and military organizations to collect information for cyber- and conventional attacks, and it is used to compromise the infrastructure of perceived enemies.

Additionally, rules for engagement in cyberspace as well as cyber strategies are currently developed by military institutions or institutions doing military research. The *Tallinn Manual* (Schmitt 2013) endeavors to apply international law of armed conflict on the cyberspace (for details see below). National military authorities, e.g., the German federal army, *Bundeswehr*, develop international rules and national strategies for conflicts in cyberspace (see, e.g., the cyber strategy documents of the German ministries of interior and the German ministry of defense (Federal Ministry of the Interior 2011; Netzpolitik.org 2015; Federal Ministry of Defense 2016).

Such cyber strategies are enacted to deal with the perceived threat caused by hostile cyber activities. According to the strategic guideline of the German federal ministry of defense, five fields of action have to be considered when implementing a cyber strategy (see Netzpolitik.org (2015)):

- A cyber security strategy must contribute to the security precautions of the nation in general.
- It has to contribute to an international security framework.
- Cyberspace must be considered a military operation space in its own right.
- Chances of cyberspace should be benefitted from.
- Risks of cyberspace should be dealt with appropriately.

The strategy described in Netzpolitik.org (2015) requires the provision of instruments to restrain the enemy in using his military capabilities and resources, or even fully prevent him from doing so. Measures may be employed to disturb information and communication systems. It is also stated that offensive abilities may be seen as a complementary, supporting, or substituting instrument to affect targets at adverse military sites. Offensive cyber weapons are considered to have the potential to extend the range of effects of the federal army in multinational endeavors significantly. Exploiting this potential obviously is part of the strategy – in spite of the fact that offensive action violates international law.

To deal with the threats emerging from potential enemies' growing cyberwar capabilities, it is planned to extend and enhance own cyberwar capabilities. For

example, the German federal army intends to build up the new CIR (Cyber- und Informationsraum / cyber and information space) command – a new department in the ministry of defense, on the same organizational level as the existing departments: air force, navy, and land forces. Suggestions are made for recruiting staff for military and civil tasks – this includes cooperation with universities.

Despite the organizational classification of the cyberspace often used – e.g., in the German cyber defense strategy – (Carr 2012) considers the approach to classify cyberspace as another domain like air, land, sea, and space, a common mistake policymakers make. Instead, he considers it some kind of "parallel universe," existing in parallel to the physical world, being able to influence it in different ways. He definitely rejects the notion of cyberspace as something similar to physical space.

The Attraction of Cyberwar

Cyberwar seems to be quite attractive from a military and political point of view. Whereas the development of very sophisticated cyber weapons like the Stuxnet is extremely expensive, the development of ordinary cyber weapons is comparatively cheap and easy. One needs some good programmers or hackers and some powerful computers. A cyber attack does not endanger the life of the own soldiers directly and immediately as in conventional attacks. Moreover, cyber attacks are not easily traced back to the attackers, it is often even impossible to identify the origin. Cyber attacks may cause severe damage on the civil infrastructure of the adversaries so that they are significantly weakened before they can strike back. But the seemingly advantages are disadvantages at a closer look. As simple cyber weapons are cheap and easy to get, many states including small and poor ones as well as terroristic organization can afford them. The proliferation of cyber weapons is impossible to stop or keep at bay at least. Today's state of information and communication technology causes the paradoxical phenomenon that it is much easier to perform cyber attacks than to prevent them. As the targets of cyber attacks are ICT-based systems, the highly developed countries are much more endangered than developing ones. Hence, one may wonder why the highly developed countries favor and push cyberwar capabilities although they might be the first to suffer severe damage.

The Cyberarms Race Increases the Danger of War

A particularly frightening aspect of the cyberarms race is the possibility that the general danger of and readiness for war increases. As the availability of cyber weapons is high and the costs are low, many potential aggressors can afford them and the threshold of their use is low. But it is even more dangerous that cyber attacks may lead to counterstrikes with conventional weapons. Cyberwar cannot be restricted to the mutual destruction and disruption of computers and ICT-based infrastructure. It must be feared that cyberwar might lead to a general war.

For example, various passages of the Department of Defense Strategy for Operating in Cyberspace (Department of Defense 2011) read like the following one with a foreboding undertone:

"The potential for small groups to have an asymmetric impact in cyberspace creates very real incentives for malicious activity. Beyond formal governmental activities, cyber criminals can control botnets with millions of infected hosts. The tools and techniques developed by cyber criminals are increasing in sophistication at an incredible rate, and many of these capabilities can be purchased cheaply on the Internet. Whether the goal is monetary, access to intellectual property, or the disruption of critical DoD systems, the rapidly evolving threat landscape presents a complex and vital challenge for national and economic security" (confer also the next subsection on the Tallinn Manual).

A thrilling question in this context is whether a cyber attack against one of the NATO members will trigger the case of alliance.

Cyberwar and the International Law of War

It is an ongoing discussion, how the principles of international law of war must be appropriately applied to armed conflict in cyberspace. In 2013, the NATO Cooperative Cyber Defense Centre of Excellence located in Tallinn, Estonia, published the Tallinn Manual (Schmitt 2013), which systematically endeavors to compile and transfer existing regulation for cyber armed conflict, derived from international law of war, to cyberspace. Another important topic that will be considered briefly, induced by the drone war conducted mainly by U.S. military forces in the Middle East, is the legal assessment of drone killings, where a debate between military institutions and non-governmental organizations on its justification – legally and ethically – is in progress.

Tallinn Manual

The Tallinn Manual defines a cyber attack as *"... a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"* (Schmitt 2013, Tallinn Manual). It consists of seven areas of legislation:

- *States and Cyberspace*, which deals with topics like sovereignty, jurisdiction, and responsibility of states
- *The Use of Force*, where the use of offensive force by means of cyber operations is stated unlawful, and the right to self-defense and the rights of international governmental organizations to take action in international conflicts is asserted
- *The Law of Cyber Armed Conflict*, where international armed conflict is characterized as a situation where hostilities including cyber operations take place; also the criminal responsibilities of commanders and superiors for ordering cyber operations constituting war crimes is reaffirmed
- *Conduct of Hostilities*, where participation and combatant status of an armed cyber conflict are defined, a definition of cyber attacks, rules for (cyber) attacks

against persons and objects, means and methods of cyber warfare, conduct of attacks, precautions, and improper use (including espionage)
- *Certain Persons, Objects, and Activities*, which deals with specific rights of certain groups of persons, such as medical personnel, journalists, or children but also with the protection of the natural environment and cultural property in an cyber conflict
- *Occupation*, where the rights of an occupying power in a cyber conflict is determined
- *Neutrality*, where restrictions of operations on neutral territory and infrastructure are determined

Basically, the Tallinn Manual transfers the common rules of international law of war to the cyberspace and to cyber operations conducted therein. It applies the same principles on cyber warfare as commonly known in armed conflict in general.

An important topic in this field is: Which are the circumstances that define cyber operations an act of war? From the Tallinn Manual authors' point of view, cyber operations are already acts of war, if they are conducted by civil institutions, and governmental authorities take no measures to prevent them from these operations. If cyber operations cause "significant" damage, defenders are authorized to conduct a conventional military response. This is criticized, among other reasons, with reference to the attribution problem (Johnigk and Nothdurft 2015), which makes it hard to determine the actual originator of a drone attack.

Currently, the second edition of the Tallinn Manual is in preparation and expected to be published soon.

Drone Killings

A particular challenge in the field of international law of (cyber) armed conflict is the topic of drone attacks: When is it justified by international law of war to kill humans by drone attacks? The answer to this question mainly depends on the definition of "combatant." In Zimmermann (2013), the topic is discussed, if the assumed definition of the US military, all male persons of a certain age encountered in a combat area, possibly carrying a weapon, may be considered a combatant and therefore can be legally killed. This definition might be too broad, so it is questionable, if it can be legitimately applied. In its broadness, it is not accepted by most nongovernmental human rights organizations.

Moreover, drone killings also take place in Pakistan, which is not party in the Afghanistan war. In Zimmermann (2013) the possibility is discussed, if the combat zone can be extended to parts of northern Pakistan and so drone killings are also legally justifiable in this area.

The different definitions of combatant obviously lead to different figures of legally killed combatants and "collateral damage." While the US government, due to its broad definition of combatant, considers collateral damage very low, nongovernmental organizations consider it unacceptably high. (On casualty figures in the Iraq, Afghanistan and Pakistan wars, partly due to drone killings, refer to (IPPNW 2015)).

The Technological Aspects of Cyberwar

The cyberspace has got much attraction for military strategies since it is the only domain where military operations can still be kept secret. Paradoxically, since the cyberspace has become the ultimate medium to spy on the entire world so that it is no longer possible to hide conventional military activities anywhere on the globe. In contrast to physical, chemical, or biological weapons development and production weapons for the cyberspace do not necessitate conspicuous facilities, no physical space is needed for their transport and deployment, and their testing and application do not leave physical traces – while digital traces can be manipulated, veiled, or even be erased. Hence, cyberspace was established as a fifth domain for military operations, beyond land, sea, air, and nearer space, long before this was discussed in public. Still, however, our knowledge about military affairs in the cyberspace is vague, even after Edward Snowden's uncoverings. Still the range of the effects of military cyber operations cannot be sized up. The lack of knowledge makes the subject the more threatening. And for good measure the abstract and obscure nature of the matter complicates a sober public discussion.

Some Security Basics

Before going into the details, let's recall a few security basics. Implementing security starts with considering the relevant security objectives. Commonly, at least three security objectives are applied (sometimes referred to by their initials, "CIA"):

- Confidentiality: The information processed by the system must not be disclosed. Confidentiality might also be legally enforced by data protection legislation. This objective will be violated, if an attacker obtains unauthorized access to system and data.
- Integrity: The information must not be changed in an unintended way. This objective will be violated, if an attacker introduces malicious software that manipulates programs or data.
- Availability: The information processing system and the information itself must be available. A common kind of attack violating availability is the "denial-of-service"- (DOS-)attack which overloads the targeted systems and so restrains or even closes down the services it provides.

Besides these common objectives, additional objectives may be considered, such as authenticity, non-repudiation, accountability, and anonymity.

To implement an information security management system the relevant security objectives must be selected, risks must be analyzed and prioritized, and appropriate measures must be implemented. Security measures must be included in a comprehensive risk management system. Industry standards are commonly applied, such as the ISO 27001 information security management standard (ISO 27001 2013).

Vulnerability of Systems and Networks

Most scenarios of military cyber attacks are based on clandestine nonauthorized intrusion into an opponent's computers or computer networks. It's a good question why we are still unable to sufficiently protect our computer systems despite of all the effort put into computer security. To keep it simple, networked computers and computer networks are intrinsically vulnerable. Networked computers are destined for communicating. Therefore ports have to be provided to allow data to flow inside-out and outside-in. Those ports are certainly gated. But, like in our physical reality, no gate can forever be protected against fraudulent access. Since error-free systems are hard to achieve – even if one uses verification techniques, which besides are economically applicable only in a small range of high-level-security systems – there is no absolute security. The designer of computer security software has to kind of act like a chess player who has to anticipate every possible movement of the opponent. Only the play has no termination, it has no rules, and the opponent's options are endless. There will always be new kinds of threats one cannot predict, and there will always be new vulnerabilities in our systems and networks.

Moreover, the opponent's resources are enormous. There are, on one hand, the human resources, a tremendous pool constituted by the community of autonomous hackers. There are, on the other hand, the vast budgets of secret services. Known, for example, from Edward Snowden's uncoverings, the NSA runs search engines and databases which map every accessible computer worldwide, keep records of their particular software outfit and appropriate break-in tools. There are certainly further organizations to maintain similar systems. Those organizations go shopping on a prospering black market to buy from hackers, for good money, knowledge about security leaks and appropriate break-in tools ("secret services are no criminal prosecution authorities . . .") – a deal of mutual benefit.

Tools

Approaches for unauthorized intrusion into computer systems and computer networks cover a wide range. They can be roughly classified into *types* of tools and *ways* of propagation of malicious software. Types of malicious software are trojans, worms, viruses, rootkits, bootkits, backdoors, remote administration tools, cyber espionage toolkits with appropriate payload, and, finally, combinations of several of above types which yield really complex cyber attack platforms. The compilation demonstrates the variety of malicious approaches, and this list is by far not exhaustive.

Complimentary, there are also numerous different ways of propagation of malicious software such as infection of files, infection of USB drives, hard disks, and other physical media; preparation of hardware accessories such as routers or computer mice or even USB cables; social engineering (often combined with blackmailing), watering hole attacks, and finally exploits. Of all these the so-called exploits deserve a little more attention: An exploit is a piece of software that takes

advantage of vulnerability in order to cause unintended behavior of the attacked computer's operating system. The vulnerable point may be caused by a bug or by perfunctory programming.

We have, however, to face the fact that even the most careful designed software systems will never be absolutely proof against the incredible creativity of hackers to find toeholds for their exploits. Even worse, their options will get more numerous with increasing complexity of software and manifoldness of interconnections. Last but not least security is not available for free, viz., someone has to pay for security measures, so they must also be justified from an economic point of view. Hence security is often a trade-off between benefit and effort. In the end we should not (only) blame software engineers for every security leak.

An exploit enables the attacker to get unauthorized access to the attacked computer, either by capturing an existing user account or by creating an inconspicuous new one. By privilege escalation, the clandestine invader will eventually yield root permission, which gives him full control of the computer system. At that point the invader can read every file, write into files, create files, install and execute programs, and even manipulate log files. Then he can delete – or at least veil or blur – the traces of the attack. This way the attack software may be forever implanted into a computer and never be found.

This is a cyber attack, but what is the weapon in such a case? Above type of attack is rather a procedure that makes use of an appropriate toolbox. We may call it a "guided attack." The term cyber weapon would better apply to a second type of attack, a so-called unguided attack. Then a malware specimen is released into the internet – "into the wild" – to find its destination without guidance. This type of attack malware consists of a dropper and a payload. The dropper propagates through the net by infecting untold computers or media. Only when it has found its destinations, it unfolds its malicious payload. A prominent example was *Stuxnet*. The dropper was a worm, the payload's targets were specific SCADA systems, i.e., a well-established computer architecture for industrial control. Because of its complexity and elaborateness the Stuxnet approach is rated among the category of *advanced persistent threats* (APT). Recently Kaspersky Lab published their current findings of APT campaigns that were still in the wild in 2015 (in most APTs a date of expiration is implemented). Not in all cases it was clear whether those were designed for military or for criminal purposes – or possibly for both. It is interesting how parts of one specimen are passed on to others (Kaspersky 2015).

Effects of Cyber Attacks

The potential effects of cyber attacks cover a wide range. Actually, the prevailing objective of cyber attacks is espionage. Nevertheless can cyber espionage yet be classified as a kind of cyber attack since it requires forcible break-in into an opponent's cyber territory. Moreover, quite often espionage operations simultaneously serve for the establishment of hidden access paths to computers and networks for proceeding measures. Such can be to spread misinformation and

disinformation for the purpose of a destabilization of the civil population by means of breaking into the computer networks of press agencies or TV stations. More sophisticated attacks could cause effective damage by taking over full control of computers or computer networks. Digital damage could be caused by the destruction or corruption of data. The targets could be administrative computer centers and the objective would be to obstruct public administration or cripple the financial system. Even physical damage could be caused, for example, by running a computer-controlled machine into a self-destructive mode or by corrupting a chemical production line. Most threatening are potential avalanche effects. An avalanche of physical consequences can be triggered by corrupting critical infrastructures such as the public communication networks or the national electrical power grid. A review study accomplished 2010 on behalf of the German Parliament made up realistic scenarios of a long-term wide-range breakdown of the national electric energy grid (Petermann et al. 2010). It reads like a nightmare. This way a nation may be forced to their knees without employing any conventional weapons.

Beyond direct effects, a variety of mediate hazards have to be regarded. Some are due to the absence of boundaries in the cyberspace. The cyberspace has neither geographical nor political boundaries, no distinction is made between friend vs. foe, identical technologies are employed by criminals, terrorists, and military cyber commands, and military code travels through the networks side-by-side with civil code. One such effect is the causation of collateral damages (by the Stuxnet campaign, for example, up to 300,000 systems have been infected, mostly civil). Unintended release of military malware can trigger a severe conflict. Intelligence agencies go shopping on a prospering black market to buy knowledge on security leaks and exploits from criminals. By concealing their knowledge they compromise the security of civil systems intentionally. Military implementations, once released into the cyberspace, will be captured sometime or other and reengineered – not only by civil security researchers and alien intelligence agencies but also by black-hat hackers. This kind of technology transfer is mostly not desired since the unwanted beneficiaries will be opposing forces, criminals, or even terrorists. A further severe problem is made up by the de facto impossibility to attribute a cyber attack sufficiently fast to its originator (Johnigk and Nothdurft 2015). An overhasty counterattack – possibly by means of conventional weapons – could easily hit the wrong suspect and trigger an escalation of violence.

Countermeasures

This chapter is concluded with some propositions for countermeasures. Simply unplugging subsystems from the networks as often proposed (e.g., Gaycken 2011) is no ultimate solution. We know by the Stuxnet campaign that a physical gap does not constitute a forever insurmountable barrier. Usually the unplugged subsystem is still confined to the host's data realm. Program code, configuration data, log files, etc., are transferred back and forth via storage media or so-called field programming devices – which can as well be infected. Instead we should appeal to the data industry to reduce

networking complexity and to abstain from interconnecting systems wherever the risks of security leaks are not justified by a functional benefit. Similarly, we should appeal to the software industry not to squeeze too much heterogeneous functions into one system. We like to mention a simple example: Why does the control of a new high-end car need over hundred million lines of code? Compare that with the 50 million lines of code to control the Geneve Large Hadron Collider. Do they really need to mingle the control of brakes and engine with the control of the sound system and the air conditioner? Instead of investing into an additional processor chip we accept the risk of the motor control to be corrupted by means of an infected mp3 file – which has recently been reported. On a more general level, it is recommended to invest into the empowerment of cyber forensics. Complementary, software concepts should be established which support forensic investigations, which assist the tracking of attacks and the preservation of evidence. For example, a cryptographic time-stamp protocol could be made mandatory, like the X.509.

Above all, it is necessary to shake up the civil society. Awareness of the risks has to be strengthened, and behavioral changes in handling data have to be motivated. However, even the sum of all technical efforts and behavioral changes will not cope with the tremendous and manifold hazards. Backup by political action has to be demanded hence – ultimately by striving after an international ban of cyber weapons. However, warning shouts are already ringing out about the impossibility of arms control and verification in the obscure cyberspace. But then the circle closes with the statements commencing this section.

Cyberpeace

From the preceding sections one can conclude that information technology and communication infrastructures have been in the focus of military institutions and secret services from the beginning. Not only was the Internet originally introduced by US military institutions – it emerged from the *Arpanet*, named after the *Advanced Research Project Agency* (ARPA) of the US Department of Defense – it also serves as an infrastructure for military action today, being under surveillance of secret services and military agencies to gather information for cyber- and conventional military means and used for cyber attacks in order to compromise the infrastructure of the perceived enemy.

Although originally the Internet served primarily as an infrastructure for military purposes, it has changed to a network that was used for scientific and increasingly for commercial and private purposes. Thus it has become a tool for international understanding, global information, and communication. But as a medium it also poses a potential threat: through its potential for surveillance and its numerous options for military operations – fostered by national authorities – it jeopardizes national and international peace.

So, obviously, the challenges of cyberwar cannot be met solely by technical means. The need for political action leads to the concept of *cyberpeace*. Cyberpeace means to restore peace in cyberspace and so its usage for international understanding

through political measures and treaties. The risks and dangers to civil society resulting from cyber warfare require political action. An alternative model to military usage of the Internet must be developed and strengthened. The civil society must request that all kinds of cyber warfare be rejected, the integrity of the Internet be preserved, and that the Internet be used in a peaceful fashion and protected against military misuse. Additionally, each form of surveillance violating human rights must be banned. Society must defend itself against a security doctrine that sets every single human being under suspicion of terrorism. In brief: Society must advocate for cyberpeace.

While it is doubtlessly important for security authorities to deal with the threats from cyber warfare activities, and the proposal by the ministry contains important topics, most of the measures proposed must be considered a new step in an armament race and an escalation in international state politics. Instead, an alternative model of de-escalation and disarmament is proposed.

A Framework for Cyberpeace

The following sections elaborate on the framework for cyberpeace that has been developed tentatively in the cyberpeace campaign for a peaceful use of the Internet and all information and communication infrastructures of the Forum Computer Professionals for Peace and Social Responsibility (*Forum Informatiker.innen für Frieden und gesellschaftliche Verantwortung*, FIfF) (confer https://cyberpeace.fiff.de/). The framework consists of the following elements:

- Rebuilding trust, which has been seriously affected by the worldwide secret service surveillance recently disclosed. This degradation of trust seriously affects a main resource of political, social, and economic cooperation.
- Condemning offensive action and promoting nonviolent means of conflict resolution by assuring that nations are not willing, and actually cannot, carry out offensive strikes against each others' vital infrastructure, by mutual agreements and control.
- Securing vital infrastructure by technical means – building up security provisions, which prevent aggressors from infiltrating computer networks and computer systems, which are vital for the supply of a society with basic services, as energy, health care, communication, etc.
- Preserving political control, democracy, and security by a cyberpeace initiative on government level, democratic control of the Internet, and cyber security strategies and ensuring a demilitarized political language.

Rebuild Trust

Our society is based on trust – this is what sociologist Niklas Luhmann pointed out in his book *Vertrauen* ("Trust") in 1968 (Luhmann 2000) – long before the Internet

arose to influence our entire life. Luhmann points out that trust is essential to reduce the social complexity of our societal environment. This is necessary to enable us to take all the decisions everyday life requests us to. With a lack of trust, the number of decisions to take would become overwhelming, therefore, we would not be able to cope with everyday life. Security expert Bruce Schneier (Schneier 2012) illustrates this convincingly:

"*Just today, a stranger came to my door claiming he was here to unclog a bathroom drain. I let him into my house without verifying his identity, and not only did he repair the drain, he also took off his shoes so he wouldn't track mud on my floors. When he was done, I gave him a piece of paper that asked my bank to give him some money. He accepted it without a second glance. At no point did he attempt to take my possessions, and at no point did I attempt the same of him. In fact, neither of us worried that the other would. My* wife *was also home, but it never occurred to me that he was a sexual rival and I should therefore kill him.*"

Using Internet services also requires trust – and we are commonly willing to provide this trust, for instance, by calling up web sites, often without double-checking their trustworthiness. We often simply rely on our intuition. We call up web sites without encryption, trusting that nobody would eavesdrop on our communication. Also, we do not encrypt our e-mail – nobody would read along and if so, what could possibly happen?

The recent disclosures should have changed our minds. Edward Snowden provided us with the consciousness of worldwide surveillance of the entire communication by secret services (Greenwald 2014). Josef Foschepoth (2012), Professor of history from the University of Freiburg, made clear that modern mail and communication surveillance started from the end of Second World War – not only in the eastern states but also in the Federal Republic of Germany. An inquiry committee of the German parliament was appointed to investigate unconstitutional surveillance by the *German Federal Intelligence Service* (Bundesnachrichtendienst) (German Bundestag 2014).

Trust cannot be enforced by political claims – it grows (and vanishes) due to actual action. Nevertheless, political action is necessary to restore trust and to enforce the demands that derive from the second and third issue mentioned above.

But how can one achieve trust? Thomas Reinhold (Reinhold 2016) proposes an international network of early warning systems and to deal with critical security incidents collaboratively. One of our demands elaborated on below is the promotion of open source in order to make independent reviews of software (and hardware) possible and so prevent systems from being infiltrated with backdoors and malware.

Nonviolent Conflict Resolution Instead of Offensive Action

Real peace is only possible if all parties renounce the use of violence and the possession of arms. Since unilateral measures of disarmament lead to the risk of insufficient defense capacities, bilateral or multilateral agreements must be concluded. These agreements should aim at structural inability to attack and the

limitation of military capacity to defense. Strict rules must be agreed upon to protect people if a conflict might arise even though military strategies are focused on defense. For that reason, the following demands are put forward (Forum Computer Professionals for Peace and Social Responsibility (FIfF) 2014):

1. No offensive or pre-emptive strikes in cyberspace. Of course, each state has the right to defend itself against attacks – cyber attacks as well as conventional attacks. But one should reject any kind of offensive attacks, including pre-emptive strikes to forestall an assumed attack by a potential opponent. We request states to publicly declare to abstain from offensive and pre-emptive cyber strikes and every kind of the offensive use of cyber weapons. Economic interests should never be a legitimate reason for cyber attacks, as for instance the assumed violation of intellectual property rights. Governments shall not use cyber weapons for this purpose.
2. Exclusively defensive security strategy. Although, of course, all nations have the right to defend themselves against attacks, we are of the opinion that no nation has the right to attack. So states should maintain a clearly defensive cyber strategy; they should publicly commit not to develop nor use cyber weapons for offensive means.
3. Disarmament. Cyber weapons, as all kinds of conventional weapons, are a security threat to everyone, as they may affect all kinds of infrastructure vital to human life and wellbeing. Relying on (undisclosed) vulnerabilities, the effect of cyber weapons is not restricted to the target of an attack. Instead, it potentially affects all systems with the specific vulnerabilities exploited for this attack.
4. No conventional response to cyber attacks. We do not consider it acceptable to respond to cyber attacks using conventional weapons. This would cause an escalation of violence that might easily become uncontrollable. In addition, the attacker cannot be easily determined (attribution problem), so the risk of conventional strikes on innocent victims is high (Johnigk and Nothdurft 2015).
5. Geneva Convention in cyberspace. In a war, critical infrastructure facilities are attractive targets, since their failure would fundamentally weaken an enemy. However, the failure of infrastructure also seriously affects civil society by attacking vital facilities like water supply, energy, health care, etc. This essential infrastructure for the civil population must not be targeted. From a cyberpeace point of view, a violation of this principle should be considered a war crime. Nations and their governments are urged to commit to common principles agreed in international treaties. The Tallinn Manual (Schmitt 2013; Heintschel von Heinegg 2015) might be a start, but it would have to be reworked to emphasize the avoidance of the use of force – for instance, conventional responses on cyber attacks are possible according to the Tallinn Manual, which have to be rejected.

Secure Vital Infrastructure

Although all parties in a conflict should abstain from using military force and employ nonviolent means of conflict resolution, one must be aware that defensive military

capacity has to be built up to intervene in cases when short-term nonviolent conflict resolution is not possible and a military cyber attack takes place. Additionally, cyber attacks from nonmilitary origins have to be considered, such as cyber crime and cyber terrorism – a strongly expanding threat. Public authorities and business companies will have to take sufficient security measures and constantly update them with regard to the evolution of capacity on the attackers' side. The range spans from script-kiddies, hackers, criminals to secret services with virtually unlimited capacity to set up attacks.

From this point of view, the following demands are preconditions to make secure system operation possible – they do not guarantee it, however (Forum Computer Professionals for Peace and Social Responsibility (FIfF) 2014).

6. Disclose vulnerabilities. Cyber attacks often rely on undisclosed vulnerabilities. Vulnerabilities are employed for all kinds of cyber attacks – actual cyber attacks, which aim to destroy the infrastructure of an enemy, and each action that seeks to prepare for war, as the surveillance by secret service authorities. To accomplish this, public authorities might accept and create vulnerabilities and keep them as a secret for future use. At the same time, these undisclosed vulnerabilities might be misused for criminal means. So full disclosure of vulnerabilities is requested – within a reasonable time span. One can expect that disclosed vulnerabilities will be fixed very quickly. This will enhance public awareness and trust in defensive security strategies.
7. Protect critical infrastructure. Currently, critical infrastructures are often easy to access from the Internet, as they are connected to publicly accessible services. In some cases, it might be reasonable to connect services to the public Internet in order to enhance the accessibility and quality of public services. Nevertheless, it must be considered that vulnerabilities are unavoidable in many cases and may be employed to attack by hostile users. So the security of critical infrastructure must be verified by competent and transparent audits and tests. The operators of critical infrastructure must be obliged to protect this infrastructure from cyber attacks. They must be obliged to implement and operate secure systems. They must not rely on state authorities or even the military. Wherever possible, critical infrastructure – like nuclear power plants – must be separated from the public Internet.
8. Establish cyber security centers. Facilities are required which ensure that threats from cyberspace can be effectively dealt with and which implement appropriate instruments to provide and enhance cyber security. They must be organized in a way that preserves fundamental civil and human rights. Additionally, they must be consequently peace-oriented and work in a transparent fashion. Separation between police, intelligence, and military authorities must be provided.
9. Promote (junior) IT experts. Today, there is a lack of IT experts and knowledge for effective protection from cyber attacks in Europe. This is even increased due to IT experts working for compromising IT systems instead of improving their security. So the quality of IT products – particularly with regard to IT security – must be enhanced significantly to reduce their vulnerability. Governmental

authorities and economic enterprises should invest in qualified IT junior experts in general and IT security in particular. Academic education must be broadened to cover ethical and political aspects as well as the assessment of technological impact.

10. Promote Open Source. In contrast to proprietary software, open source software may allow independent inspections and reviews. This is expected to reduce the probability of undisclosed backdoors significantly. In principle, the entire community can conduct these reviews. So open source software should be promoted and used by governmental authorities. It should be preferred particularly for critical infrastructure. Governmental authorities should also promote independent reviews and inspections. Nevertheless, we have to be aware that open source is not the solution to all security challenges – it is not sufficient that it is virtually possible to inspect systems and find its vulnerabilities – but that reviews must be conducted in practice by competent reviewers, and sufficient resources must be granted to achieve the necessary effort. But still, there is no guarantee to eliminate all vulnerabilities critical to confidentiality, integrity, and availability of the systems.

Preserve Democratic Political Control

The demands mentioned before need sufficient attention on the political level. Organizational and legislative measures must be taken to promote confidentiality, integrity, and availability; bring forward democratic control and civil rights such as free speech; and, last but not least, take care of appropriate political language (Forum Computer Professionals for Peace and Social Responsibility (FIfF) 2014).

11. Cyberpeace initiative on government level. From this point of view, the cyberspace – i.e., all kinds of critical communication infrastructure – is a vital basis for the future of mankind. So endangering the integrity of this critical infrastructure means jeopardizing our future. A cyberpeace initiative must be launched to preserve the confidentiality, integrity, and availability of the communication infrastructure. Peace studies and the development of peace-keeping strategies in cyberspace should be promoted.
12. Democratic control of the Internet and cyber security strategies. Today, cyber strategies are developed and implemented secretly. Meanwhile, only transparent cyber security strategies can be confidence-building measures and counteract an armament race in cyberspace. So democratic control and separation of powers are required. Parliamentary approval for cyber security strategies and their implementation must be mandatory. Cyber security strategies should be an outcome of legislative democratic decision-making. They have to be controlled by a division of powers.
13. Online protest is not a crime. Information and communication via the Internet nowadays is common practice. So to exercise fundamental rights – e.g., free speech – must not be considered a crime. Especially, it must not serve as a reason

for military response or war as well. Examples are consumer protests against online services. The right of civil disobedience and online protest has to be respected. Online protest must not be criminalized or even serve as a reason to start a war.

14. Well-defined and demilitarized political language. Finally, politics and media frequently use vague language with the effect of potential escalation of conflicts. For instance, using the term "cyberwar" might suggest that only military solutions are possible. Cyber crime, in contrast to cyberwar, must be targeted by criminal law rather than by military means. This has to be reflected in political language.

These four fields – trust, nonviolent conflict resolution, securing vital infrastructure, and democratic political control – are considered an appropriate framework to achieve cyberpeace. The framework with its 14 demands should help to take the political decisions to reject the military colonization of the Internet, promote peace and human and civil rights in cyberspace.

Conclusion

In the first two sections of this chapter, we have sketched some significant aspects of the growing threat of cyberwar. The first section has been concerned with the military and political issues of cyberwar from the problematic notion over the endangerment of the civil society to cyber strategies and the international laws of war. The second section has focused on the technological aspects including security basics, the vulnerability of information and communication systems, and the tools of cyber attacks. As a counter-part of cyberwar, the third section has outlined the framework of cyberpeace covering the issues of rebuilding trust, resolving conflicts in a nonviolent way, securing vital infrastructures, and preserving democratic political control.

The future investigation of the technological and political aspects of cyberwar and cyberpeace may put the topic into the larger context of knowledge economy and knowledge society (see, e.g., (Powell and Snellman 2004; Bindé 2005; Rooney et al. 2005)) where knowledge economy refers to the observation that economy is more and more transformed from labor-oriented to knowledge-intensive, and the idea of the knowledge society advocates a fair access to knowledge as the base of future politics, culture, and prosperity. But there are also risks. Espionage and sabotage are military measures as long as wars have been conducted. The technology of weapons reflects usually the highest technological state if it was not the driving force. All this has reached a new quality in the connection of cyber warfare as the use of information and communication technology opens new possibilities of worldwide surveillance, collection and analysis of big data, and of the destruction of civil infrastructure through the infiltration of the underlying computers and networks, In this sense, one may look at cyberwar as the dark side of the knowledge society and knowledge economy.

The ultimate goal of cyberpeace is a ban of cyber weapons and a fully civil Internet in particular. The ban is demanded not only because the danger of conventional military conflicts is immensely increased by the running cyber armament race but also because the critical civil infrastructure in highly developed countries in particular may be destroyed with unforeseeable economic damages and even a great number of fatal victims.

Reference

Bindé, J. (Coord.) (2005). *Towards knowledge societies: UNESCO world report* (UNESCO reference works series). Paris: UNESCO. http://unesdoc.unesco.org/images/0014/001418/141843e.pdf. Accessed 27 February 2017.

Brenner, S. W. (2009). *Cyber threats: The emerging fault lines of the nation state*. Oxford, UK: Oxford University Press.

Carr, J. (2012). *Inside cyber warfare* (2nd ed.). Beijing etc: O'Reilly.

Clarke, R. A., & Knake, R. (2012). *Cyber war: the next threat to national security and what to do about it*. New York: HarperCollins.

Costigan, S. S., & Perry, J. (2012). *Cyberspaces and global affairs*. Farnham, Surrey: Ashgate.

Department of Defense. (2011). Department of defense strategy for operating in cyberspace. http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. Accessed 25 July 2016.

Federal Ministry of Defense. (2016). Abschlussbericht Aufbaustab Cyber- und Informationsraum. http://www.bmvg.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5NmU2ODYyNzc2MzY5NzMyMDIwMjAyMDIw/Abschlussbericht%20Aufbaustab%20CIR.pdf. Accessed 21 July 2016.

Federal Ministry of Justice and Consumer Protection. (2001). Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ("G10-Gesetz") http://www.gesetze-im-internet.de/g10_2001/. Accessed 21 July 2016.

Federal Ministry for Justice and Consumer Protection. (2012). Basic law for the federal republic of Germany. http://www.gesetze-im-internet.de/englisch_gg/. Accessed 21 July 2016.

Federal Ministry of the Interior. (2011). Cyber-Sicherheitsstrategie für Deutschland, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile. Accessed 21 July 2016.

Forum Computer Professionals for Peace and Social Responsibility (FIfF). (2014). Forderungen zum Cyberpeace. *FIfF-Kommunikation, 31*(4), 62–65.

Foschepoth, J. (2012). Überwachtes Deutschland. In *Post- und Telefonüberwachung in der alten Bundesrepublik*. Göttingen/Bristol: Vandenhoeck & Ruprecht.

Gaycken, S. (2011). *Cyberwar. Das Internet als Kriegsschauplatz*. Munich: Open Source Press.

Gaycken, S. (2012). *Cyberwar – Das Wettrüsten hat längst begonnen*. Munich: Goldmann/Randomhouse.

German Bundestag. (2014). 18th electorial term: Establishment of a committee of inquiry; Printed paper 18/843. http://www.bundestag.de/blob/284528/a89d6006f28900c4f46e56f5e0807ddf/einsetzungsantrag_englisch-docx-data.pdf. Accessed 25 July 2016.

Greenwald, G. (2014). *No place to hide. Edward Snowden, the NSA, and the US surveillance state*. New York: Metropolitan Books.

Heintschel von Heinegg, W. (2015). Völkerrecht im Cyberraum – das Tallinn-Handbuch und der Tallinn-2-Prozess. *Dossier 79*, *W&F Wissenschaft und Frieden 3/*2015 *& FIfF-Kommunikation* 32(3).

Hügel, S. (2016). Cyberpeace – Promoting human rights and peaceful use of the internet. In Hofkirchner, W. & Burgin, M. (Eds.). The future information society, Singapore: World

scientific, to appear. (A short version can be found under: http://cyberpeace.fiff.de/Uploads/Uploads/ISIS_Cyberpeace_Extended_Abstract.pdf).
IPPNW – International Physicians for the Prevention of Nuclear War (2015). Body count. Casuality Figures after 10 Years of the "War on Terror" 1st international edition. Washington DC., Berlin, Ottawa. http://www.ippnw.de/commonFiles/pdfs/Frieden/Body_Count_first_international_edition_2015_final.pdf. Accessed 24 July 2016.
ISO 27001 (2013). ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization.
Johnigk, S., Kreowski, H.-J., & Nothdurft, K. (2014). Cyberwar – Schimäre oder reale Bedrohung? *FIfF-Kommunikation, 31*(4), 74–76.
Johnigk, S., Nothdurft, K. (2015): Das Problem der Attributierung von Cyberangriffen und seine Folgen. *Dossier 79*, *W&F Wissenschaft und Frieden 3*/2015 *& FIfF-Kommunikation* 32(3).
Kaspersky (2015). Targeted Cyberattacks Logbook, https://apt.securelist.com, Accessed 17 July 2017
Luhmann, N. (2000). *Vertrauen* (4th ed.). Stuttgart: Lucius & Lucius.
Netzpolitik.org. (2015). Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg. https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#Strategische-Leitlinie-Cyber-Verteidigung. Accessed 21 July 2016.
Petermann, T. et al. (2010) Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung. Technological Impact Assessment Office at the German Parliament, Report No. 141, November 2010, http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsberichtab141.pdf. Accessed 26 Jan 2017.
Powell, W. W., & Snellman, K. (2004). The knowledge economy. *Annual Review of Sociology, 30*(1), 199–220.
Reinhold, T. (2016). Die Bundeswehr zieht ins Cyberfeld. *Blätter für deutsche und. Internationale Politik, 7*(16), 17–20.
Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32.
Rooney, D., Hearn, G., & Ninan, A. (Eds.). (2005). *Handbook on the knowledge economy*. Cheltenham: Edward Elgar Publishing.
Scahill, J. (2015). *Germany is the tell-tale heart of America's drone war*, The Intercept. https://theintercept.com/2015/04/17/ramstein/. Accessed 21 July 2016.
Schmitt, M. N. (2013). *Tallinn-manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press.
Schneier, B. (2012). Liars & Outliers. In *Enabling the trust that society needs to thrive*. Indianapolis: Wiley & Sons.
Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford: Oxford University Press.
Stiennon, R. (2010). *Surviving cyberwar*. Lanham: Government Institutes.
Stiennon, R. (2015). *There will be cyberwar: How the move to network-centric war fighting has set the stage for cyberwar*. Birmingham: IT-Harvest Press.
Tallinn Manual. Wikipedia entry, https://en.wikipedia.org/wiki/Tallinn_Manual/Tallinn_Manual. Accessed 24 July 2016.
Ventre, D. (Ed.). (2011). *Cyberwar and information warfare*. London/Hoboken: Wiley-ISTE.
Ventre, D. (2016). *Information warfare* (2nd ed.). London/Hoboken: Wiley-ISTE.
Zimmermann, A. (2013). Es gibt keinen rechtsfreien Raum (Interview). *Internationale Politik, 68*(3), 26–31.

Privacy in the Cyberspace: Threats and Prospects

43

Tomáš Sigmund

Contents

Abstract

This paper deals with the topic of privacy in the cyberspace. It answers the question: What is the situation regarding privacy in the cyberspace and what new threats privacy faces in the cyberspace? It starts with the specification of privacy and analyses the new situation the development of information technologies has put us in. Our environment has changed and privacy is affected. The article continues with the analysis of the threats to privacy emanating from the new environment. The threats include violation of autonomy, lack of freedom and free decisions, insecurity, information asymmetries, blackmailing, vulnerability, physical and mental suffering, financial and other losses, harms to reputation, etc. Further, the paper identifies how privacy is threatened by new technologies and

T. Sigmund (✉)
Department of System Analysis, University of Economics, Prague, Czech Republic
e-mail: sigmund@vse.cz

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_42

technological inventions. To illustrate possible impacts of information technologies on society, three dystopian visions are presented, namely Orwell's depiction from the novels *Nineteen Eighty-Four*, Kafka's *The Trial*, and Huxley's *Brave New World*. They present three deterrent examples of social reactions to the options provided by the new information technologies. The first one is unfriendly totality, the second one consists in nontransparent society, and the third one in voluntary surrender of privacy. To evaluate current situation, the legal regulation of privacy in EU and USA is summarized.

Keywords
Privacy · Information technology · Knowledge democracy · Autonomy

Introduction

The etymology of privacy teaches us that it comes from the Latin adjective privatus which meant set apart, belonging to oneself, peculiar, personal (Harper 2001). The old Greek word for this concept was "idios." In old Greece, privacy was considered something deficient, because it lacked the public aspect. Private should be considered in relation to the concept of the public as they are closely related. "Idiotes" meant a layman, a person lacking professional skill practicing his unskilled work on his own and not participating in the public affairs. For the old Greeks, the participation in the life of the society, in its politics, was praised the most. The private affairs like family life, economic activities, etc. were performed, too, but they were not public and the public sphere was not interested in them.

Today the situation is very different. The political life has changed from pursuing the interest of the state or from focusing on the object of discussion to pursuing private interests (see, e.g., Sennet 1977). The consequence of this was that private affairs became public and politicians became interested in citizens' private affairs which became related to their interests.

The distinction between private and public has changed and from the content differentiation between private and public sphere remained only the formal or structural criterion of amount of people having right to access to the information on a person. Moreover, various cultures have different understanding of privacy. For these reasons, it is difficult to find a common denominator both regarding different time periods and different areas and the formal general definition prevails even though it can't reflect the substantial differences between various privacy concepts.

Private should be distinguished from the intimate. Private realm includes the intimate, but can't be limited to it. Intimacy has relation to the body, to its vulnerability and proximity. Private is also not identical with the secret. Private matters needn't be secret, as in the example of one's haircut, but can be as is the case of one's religion.

An example of the formal definition of privacy can be found in Rössler's book on privacy (2004). According to Rössler (2004), the meaning of the concept "private" refers to actions, as in the example of voting for someone in the ballot, to certain

knowledge, like one's state of health and to spaces like one's home. Further, we can distinguish two semantic models of the term "private." We can differentiate various levels and degrees of privacy, starting from the intimate sphere and ending with the private enterprise which is protected from the state interventions. The second model refers to actions and decisions which individuals make freely anytime and anywhere without interventions and influences of the state and wide public. An example may be profession of a religion.

Rössler criticizes the definitions of privacy for their limited understanding of the concept and essentialism (Arendt and her naturally defined privacy – Arendt 1958), or too broad understanding (the right to be left alone) or imprecise (inaccessibility of a person) or a narrow concept (control of information, protection from public view). She suggests to define something as private if one can control access to it. To avoid misunderstanding, she interprets the verb "can" normatively as should/can/may. She further differentiates between decisional, informational, and local dimension of privacy. The content of these realms is according to her conventional and often open to discussion.

I'd like to raise two objections. First, her attempt to find a common universal definition of privacy doesn't allow to see the substantial differences between various privacy conceptions. Second, I don't think everything is conventional as Rössler thinks. The human body always plays a role in privacy as one has a close and intimate relationship to it. That implies we can differentiate various degrees of privacy and to the highest degree, the access and influence is restricted to everybody except the respective person and so is valid in every other sphere. The reference to "control" may also be interpreted as having something under control and in one's power. Rössler claims privacy is important for the development of autonomy and that is why control is a feature of privacy. She considers civil liberties to be insufficient for the protection of autonomy and that is why we need protection of privacy which is important for the development of autonomy which is the telos for freedom. She differentiates three types of freedom: Decisional privacy for autonomous action and decision, informational privacy that limits the knowledge of others, and local privacy which provides space for self-invention, self-presentation, love, and justice.

However, control refers just to the person and doesn't include the social aspect of privacy. Privacy doesn't mean exclusion of the general public, but also inclusion of close people and sharing with them. General public is not excluded because somebody has control over access to private matters, but because the topic doesn't include them; their relationship is different to what the context requires. The fact that something is not designated to the wide public is a feature of private matters. Having something under control is a liberal consequence of stressing the free character of man, but disregarding the power of the private matter and norms derived from it.

Privacy has also an intrinsic value, is important for the development of personal relationships and protects personhood (see, e.g., Moor 1990). Forgetting the content, aspect of privacy establishes a threat as it doesn't force to compare various privacy definitions. In every social structure, there is a differentiation between private and public or more private and more public, but that doesn't mean their delimitation is

acceptable. For example, under surveillance, people invent methods to keep their privacy, like a secret language, allegories, etc. The public sphere has changed and the private reacts to it. Or while online and publicly accessible, one can filter incoming messages and have some privacy at work. Another example may be selling one's products as the result of private work becomes public and is publicly evaluated by the price (In the Marxist perspective the product is treated in its privacy only as its value consists in the invested labour only.).

The formal definitions hold, but we must consider the content definition as well. Content of privacy is influenced by the environment in which privacy is located.

Privacy is a relevant concept for the twenty-first century as the development of information technologies has changed the friction of information transmission and transformed the whole information environment. That has, on the one hand, allowed the rise of knowledge economy, knowledge society, and knowledge democracy, but, on the other hand, called into question old heuristics, rules, and principles related to the division of private and public sphere. Only the enlightened combination of knowledge economy and respect for the private life of citizens will allow both the economic progress and undisturbed development of citizens.

The rise of knowledge society and knowledge democracy supports the importance of knowledge for the functioning of the society. Knowledge is different from raw data and a knowledgeable person respects the private sphere of other people, which is necessary for the proper functioning of knowledge democracy. Democracy needs some principles governing its functioning and one of them is the respect for privacy. That is important for the smooth functioning of the public sphere. It can then contribute to the progress of knowledge economy. Otherwise, we would be facing loss of citizens' autonomy and would be on the way to totality without the benefits of knowledge sharing and inspiring.

New Privacy Environment

With the development of media, especially the easily reproducible media, starting with the press in the seventeenth century, followed by photography in the nineteenth century, film in the twentieth century and ICTs in the twentieth and twenty-first century, the problems with the privacy of information has become quite acute. The spreading of information, its acquisition, and storing made possible by the new media has become easy with the consequence of easy breaking the privacy sphere. Today we are not far from what Foucault has described with reference to Bentham's panoptic society where every information can be controlled and observed. Foucault reminds that every right and claim we are entitled to enjoy in the just society is counterbalanced with the measures of control and observance that guarantee them.

The technological devices, especially the ICTs, threaten privacy and change the environment man lives in. The digitalized content stored in databases, Internet surveillance, big data, medical records, information about financial transactions make control over information and respect for privacy more difficult than before.

Information can be stored, analyzed, manipulated, transported, concealed, etc. very easily. Technology makes life easier, releases from many necessities, but brings new threats with itself. That is why privacy becomes topical for many legal discussions and becomes protected by law more than before.

Current cybersociety puts man into a new environment which he is not used to. Information flows independently from their producers and live an independent life. In the cyberspace, the relevance of one's body diminishes with the effect of increasing anonymity. The amount of information available is enormous, much bigger than before and bigger than a human being can understand. Moreover, media in their effort to be attractive and to achieve their aims use and misuse techniques based on deeply rooted habits and ways of behavior which people have difficulties to resist. It concerns the application of behavioral patterns based on authority respect, induction of reciprocity, impression of scarcity, fear of change, group effects, etc. Media attempt to induce emotions as emotional information tends to find way through the information noise to the recipient better than the rational one. The result is that people are exposed to so many emotional information that they become desensitized, they are overloaded with information and their decisional power is paralyzed, can't choose the correct information, simplify things. They can also get narcissistically stuck in their virtual world, lose respect and carefulness for external privacy threats. The virtual environment allows creation of unnatural world where man has difficulties to react as his mind has developed in different circumstances. That poses threats to the privacy sphere which can be attacked from many sides and man is not able to protect himself.

Floridi's Infosphere

According to many theories, ICTs make problems with information privacy worse because of their increased processing capacities and their speed, quantity, and quality of data they can collect, record, and manage. However, ICTs not only worsen the situation, but also have potential for privacy increase and for its change. In Floridi's opinion (2005), ICTs reformulate information privacy. Floridi provides some illustrative examples: many transactions like banking or booking are carried out remotely, the amount of anonymous interactions grows, digital information is volatile and fragile, digital data can be encrypted. ICT allows for both increase and decrease in information privacy. But also the informational environment has changed. Floridi defines information privacy as a function of the ontological friction (forces that oppose the information flow in the infosphere). As ICTs transport information, they are the most influential factors affecting information privacy. Factors affecting the friction can be changes in the environment or changes in the affected actors or their behavior. Old nondigital ICTs like printing, mass media, etc. tended to reduce the friction in the society because they enhance and augment the agents embedded in it. The digital ICTs create new environment or as Floridi puts it they "re-ontologize it." Floridi (2005, pp. 189–190) distinguishes five fundamental trends in the re-ontologization of information privacy:

- digitalization of informational environment
- homogenization of the processor and the processed (digital content is processed by the digital tools)
- evolution of digital agents (people equipped with notebooks, cameras, and smartphones which can freely and effectively operate in the new environment)
- informatization of interactions
- mutation of old agents into digital agents

Privacy in the Re-Ontologized Infosphere

The friction in the infosphere is importantly affected by the technological innovations and social developments. Old ICTs enhance friction and augmentation of agents and decreases information privacy, whereas digital ICTs not only decrease or increase information privacy, but also change our understanding of it. Digital ICTs have in contrast to analog ICTs the advantage of easy reproduction and technological processing.

Floridi (2005) supports the individual responsibility for information privacy where an individual constitutes his informational identity. The right to information privacy can be understood as a "right to personal immunity from unknown, undesired or unintentional changes in one's own identity as an informational entity, either actively – collecting, storing, reproducing, manipulating etc. one's information amounts now to stages in cloning and breeding someone's personal identity – or passively – as breaching one's informational privacy may now consist in forcing someone to acquire unwanted data, thus altering her or his nature as an informational entity without consent" (Floridi 2005, p. 195). There is no difference between one's informational sphere and one's personal identity. We can say "I am my information." Another consequence is that if someone's personal identity is stolen, there is another person (the thief) whose identity has been enhanced. It shows how the industrial conception of information has changed. On the other hand, that also shows how vulnerable we have become with the transformation of our lives into the infosphere.

Threats and Harms to Privacy in the Cyberworld

Floridi's conception of information privacy may seem acceptable at first sight, but similarly to Rössler it emphasizes man's responsibility only. Even if we accept man's responsibility for his privacy and its determination, we mustn't forget to analyze the situation in more detail. The individual man's power is limited compared to the big ICT companies and the state. Privacy has to be protected as it is valuable. Its values and benefits can be harmed. These aspects were analyzed by Gavison (1980), van de Hoven (2001), and Solove (2006). They focus on the Euro-American autonomy-based conception of privacy.

Ruth Gavison (1980) names some values served by privacy: healthy, liberal, democratic, and pluralistic society; individual autonomy; mental health; creativity; and the capacity to form and maintain meaningful relations with others. She also

mentions links of privacy to mental health, autonomy, growth, creativity, and the capacity to form and create meaningful human relations.

In the area of cybersociety, van de Hoven (2001) distinguishes four types of reasons why privacy should be protected: (1) information-based harm, (2) informational inequality, (3) informational injustice, and (4) encroachment on moral autonomy. They consider wider consequences of privacy harms and concentrate more on privacy than on the effects on the individual.

People can be harmed by making use of their personal information. The resulting violations can refer to financial and physical damages even though it is based on privacy violation. The more data and digital information is used, the more vulnerable the citizens become. Information is a strong weapon that can be used in many ways.

Informational inequality concerns equality and fairness. In current society, people seem to prefer the comfort of electronic communication and surrender their privacy in exchange for that. The service providers support that tendency with benefits for privacy renouncement. People agree to the use of their private information in exchange for some "free" service or product. However, the information asymmetry is in this area quite big. Many consumers don't understand the contracts in which they sell their personal data; the environment is not transparent and fair.

Informational injustice concerns the value and meaning of information which should in van de Hoven's opinion respect the boundaries of a sphere, access to the information should accommodate to local meaning. For example, medical records should be used for medical purposes; they can be accessible to the close relatives and should be used to cure the person. They shouldn't be used to discriminate, to refuse some commercial services, deny social benefits, etc. Using information across the spheres is also problematic, like when the library would recommend books based on the medical records to reduce cholesterol. Informational injustice is thus disrespect for boundaries of spheres of justice or spheres of access. Data shouldn't be transferred across these boundaries. The easy violation of boundaries between separate social spheres or areas of meaning is an important feature of ICTs. Every sphere has its rules and regulations which can be sometimes determined by empirical investigation only, sometimes they are intuitive only.

Encroachment on moral autonomy is a privacy matter in the strict sense. Lack of privacy may result in normative pressure of the community on its member. The judgments made on someone may change his view of himself and may encourage him to behave differently. The idea of autonomy and conception of a person as an author of his moral personality is the reason for his data protection.

Eric Descheemaeker (2015) differentiates three types of harms or detriments to privacy. They involve (1) pecuniary loss, (2) mental distress, and (3) the loss of privacy itself. They refer to the harms caused directly to the subject. The pecuniary loss is very obvious. It is often related to unauthorized use of private information like photographs. The financial loss is a consequence of another wrong – e.g., breach of confidence which is included in privacy. Mental distress is an unpleasant emotion caused by privacy harm. Only the third type consists in the injury of someone's privacy as such.

However, how much privacy is necessary to provide its values? We can't conclude privacy guarantees autonomy, as autonomy requires heteronomy as well to have something to differentiate from. In addition to that, there are other valuable social aspects like security, right to information, public interests, learning and education, etc., and it is difficult to find a proper balance between them and privacy. The law can provide us with some examples, but it must be interpreted by the judge, who considers specificity and context of the situation. D. Solove offers some hints in this direction. His detailed investigation of privacy harms considers relations of privacy to other aspects of social life. Furthermore, he gives examples of lawsuits where these questions were solved. That can serve as an inspiration for other cases.

Harms to Privacy According to Solove

D. J. Solove suggests in his article (2006) a taxonomy of privacy. He very aptly remarks privacy cannot be understood independently from society. However, for him privacy means relief from a range of kinds of social friction. It is a protection from activities that impinge on people (Solove 2006, p. 484). Solove identified some possible harms related to information privacy, i.e., harmful invasions into privacy. He differentiates various meanings of privacy in relation to various contexts and harms related to them. He considers uncertainty to be a big problem for privacy, harms to social relation, harms to one's identity. There are four basic groups of harmful activities: (1) information collection, (2) information processing, (3) information dissemination, and (4) invasion. Each of them has various subgroups.

The first group focuses on problems related to data subject. Into the first group belong surveillance and interrogation. Surveillance means watching or recording of someone's activities. When persistent surveillance may cause discomfort and anxiety, it may change the person's behavior through self-censorship and be an instrument of social control supporting the power of norms and regulations to an extreme extent. It may lead to mainstream behavior and discourage free innovative ideas and activities. Covert surveillance has chilling effects on behavior because the only possibility of being watched is paralyzing. Totally covert surveillance may reveal private facts that could be used to blackmail the subject.

"Interrogation includes various forms of pressuring of individuals to divulge information" (Solove 2006, p. 500). It can have the form of questioning or probing for information. The violence used in interrogation can cause harm and from a certain degree is unacceptable. Even moderate compulsion can cause offense as not answering may create the impression that the person has something to hide. Interrogated people have to consider how they will appear to others. People feel discomfort during interrogation. That may affect the freedom of association and belief. Another aspect of interrogation consists in the fact that it may cause distortion as the interrogator can control what information is revealed and how it is interpreted – it can be a form of manipulation.

The second group concerns data collectors, processors, and holders like other people, businesses, and governments. Into the second group belong aggregation,

which is the combination of various data about someone, identification, which means linking information to individuals, insecurity related to problematic use and low protection of information, secondary use meaning use of information for a different purpose than originally stated without the subject's consent, and exclusion, which consists in the fact that the person doesn't know about the data others have about him. Aggregation is dangerous because pieces of innocent information combined together become more revealing than the parts independently. Combining forms synergies. New facts may appear that are not contained in the separated data, in their combination only. The scope and power of aggregation in the information society is incomparable to the situation before. There are more data about people available, the processes and methods of combining are easier, more sophisticated and effective. Combination of data can be beneficial, but also harmful as people don't expect the results of the processing of independent data. They provide the separated data with quite different expectations. Aggregation leads to information asymmetries when some subjects are much better informed and have more power than other subjects. They can judge, evaluate, make more profound decisions, and affect one's life. Another problem related to aggregation consists in the fact that the results may be imprecise and disconnected from the real life and context.

Identification allows to connect data to a person. It enables to confirm identity. It is a sort of combination. Identification has many benefits, but also disadvantages. It creates a relatively stable connection between the person and his data. There are national identification numbers that allow to learn from their construction if the person is male or female. Anonymity and impartiality is so more difficult to achieve. Privacy can be harmed and people may feel intimidated by the revelation of personal information on them. Identification is related to interrogation, surveillance, and disclosure and so distorts and intrudes. It also creates power and control over identified person. Because it decreases anonymity, it exposes the subject to possible future harm and produces insecurity. Insecurity is related to aggregation, identification, disclosure, or distortion. To avoid insecurity, there are many rules and regulations which regulate handling and securing of information.

Secondary use is the use of data for other purposes than originally stated without the subject's consent. Not all of them are harmful, but some may cause problems. They are in conflict with what people expected and agreed as people can't expect all potential uses of data. From that it follows people giving unconditional approval to data use are in a disadvantageous position compared to the data processor. The extent of potential use creates feeling of fear, uncertainty, and insecurity. Secondary use of data is also liable to misunderstanding and misinterpretations.

Exclusion happens if people are not informed about the records of their personal data. There are reasons for exclusions like costs, legal reasons, but exclusion in any case creates insecurity, lack of accountability, sense of vulnerability, and powerlessness.

The third group of hams to privacy involves dissemination where processed data are transferred to others or disseminated. This group includes breach of confidentiality meaning breaking the promise to keep information confidential, disclosure which is the revelation of truthful information that affects the way others think of the subject, exposure which is related to someone's body privacy, increased

accessibility of information on someone, blackmail which is related to threats to disclose personal information, appropriation of someone's identity to help achieve aims and interests of another person, and distortion which involves dissemination of false information about someone.

Breach of confidentiality is different to public disclosure because it causes different kinds of injuries. Breach of confidentiality violates trust and the victim has been betrayed. In the case of public interest, it may be acceptable, but not always. Disclosure is, on the other hand, related to public disclosure of true private facts offensive to a person and is not of public concern. Disclosure harms the reputation of the person. Even though protection against disclosure limits freedom of speech and right to information, it promotes autonomy and self-development because it protects actions important for self-realization. It also supports anonymity and free associations with others. Disclosure puts a person into risk of stalking, threatening, and harassment, and increases vulnerability and decreases security. Disclosure of data without context may lead to misinterpretations and false judgments and assessments. It may threaten equality and unbalanced justice. Disclosure of someone's genetic code may put him into risk of discrimination. Disclosed information is related to secondary use. It may also connect the person with his history in an immutable way.

Exposure means exposing someone's personal physical or emotional attributes to others. Exposure reveals aspects that can't be used to judge or assess somebody, but injures the social practices we have developed to conceal animal like or disgusting activities or qualities. In certain activities like being nude or going to the toilet, we are weak and vulnerable. These norms differ, but there are always some norms regulating these activities in every society. Here privacy is understood as a space separated from civilized behavior in the public space. Revelation of these activities leads to loss of esteem, dignity, and ability to participate in society. People feel ashamed. Some forms of cyberbullying use exposure.

Increased accessibility means that information that is available to the public is made easier to access which increases the risks of disclosure. Even though there are benefits to easy accessible information, the risks can't be concealed. For example, data may be used for other than originally declared purposes for making the data publicly accessible.

Blackmail means forcing someone to do something by threats that his private information will be accessible to someone or made public. It often includes paying hush money. It is unethical and illegal because it establishes domination and control of one person over another. It involves a threat of disclosure; however, it is not the real disclosure and in that it differs from real disclosure. As Solove asserts, dominance over someone, be it slavery or blackmail, is unacceptable. The consent is in this case not voluntary.

Appropriation means that someone acts as somebody else to appropriate benefits. Personality or identity of somebody is used for goals of somebody else without its owner's will and consent. There is a commercial aspect which harms one's reputation, a property rights aspect, and a harm to freedom and self-development. The person may become publicly known without her consent. One loses control over the

way how he presents itself in the public. One's identity is shaped too much and without consent.

Distortion concerns inaccurate information on someone. It causes false or imprecise perceptions and assessments of the person by others. It is similar to disruption as it involves distribution of information that influence society's perception of a person. The result is reputational harm, domination over someone regarding the way others perceive him. The difference between distortion and disclosure consists in the fact that the spread information is false. Society is cheated and the relationships with others are distorted.

The fourth group concerns direct impingement on the individual and involves invasion into private affairs like intrusion which is the act that disturbs tranquility or solitude and decisional interference regarding private affairs. Intrusion has a relation to disclosure as disclosure is often the result of intrusion. Intrusion can have the form of physical intrusion, but also of surveillance or questioning and so has a relation to surveillance and interrogation. Intrusion causes interruption of one's activities through activities of somebody else. Spam, junk mail, and telemarketing are forms of intrusion. They consume people's time, interrupt their activities, and interrupt the solitude and safe private sphere. Everybody needs a refuge from others to have rest, develop ideas, to have a personal space around himself. Home has a privileged place among the safe places. Exclusion of the rest of society doesn't require seclusion; even in public places, man is entitled to have freedom from intrusion. Decisional interference is related to disclosure: as the resulting decision is known to the influencing party, it can use insecurity and exclusion as threats. Interference also invades the private realm which should be free from intrusion.

Solove thinks (2006, pp. 487–488) that the old privacy problems were more related to human dignity, whereas the more modern ones are more structural and involve less insult or reputational harm, but more risks that a person might be harmed in the future. He compares them to environmental problems. In the current information society, people are more exposed to the risk of harm. Many activities are monitored or simply involve some personal information and that exposes the concerned person to the risk of its misuse, victimization, etc. That causes what is called the chilling effect and involves affections in person's life. Because of permanent monitoring, people may change their behavior and may not participate in political or free activities, not because they would do something illegal, but because they would be chilled and afraid of possible misuse. Their life is changed.

The Technological Threats to Privacy

Now as we have seen what privacy is and how it can be harmed, we should map how the risks are related to modern technologies, which have allowed the development of modern information society. It can be claimed that it depends on every individual how he uses the new technologies but the fact the technological devices are available provokes and motivates the tendencies to use them in any way including those harming privacy. The advantage gained is quite tempting especially in the current

competitive market: a lot of information, better understanding of the customers and competitors, possibility to influence or even manipulate them. According to Cohen (2012) in the information society and its information economy, information is used to target advertisement, search results, to adjust pricing and risk management, to make predictions of consumers' behavior by companies as well as by the state. Surveillance and sharing of private information allows increased personalization of products and services, price discounts, better products using information from their users, more convenient access to resources and services.

Privacy is distinct from the public sphere in that it is a protected area where the elements and their relations are known and relatively predictable for the concerned person. If companies have enough private information, they can give the impression they belong into the private sphere of their customers and have good private relations with them. The customers in consequence of that decrease their attention and become easy to influence. Blurring of the private and public sphere raises a problem here because the customers' expectations are violated.

According to Julie E. Cohen (2012) privacy has a very unstable position as it has to fight against other currently important values like national security, efficiency, and entrepreneurship. Modern technologies allow close contact and easy spreading of information among people and privacy stands in this development's way. Privacy to some extent opposes the progress of knowledge.

Cohen identified two trends that make it difficult for privacy to assert its rights. One is the trend toward undisruptive invisible design and the effort to keep trade secrecy and to preserve competitive advantage which obscures and hides working of the software and network architectures. The shift leads to black box platforms. The technical complexity has made the situation worse as it is very difficult to explain how technologies work to laymen. The other trend consists in the pervasive character of surveillance technologies supported by the comfort they provide as their main feature. Efficient administration and comfortable operation of many services requires surveillance data which can be used in many ways. For example, an application recommending restaurants in the location where its user is located needs access to data about his location.

If we analyze qualities and powers of modern ICTs, we will find that they can process huge amounts of data; only a few understand how they really work as they are very complex, they don't respect any values, feel no responsibility themselves as they don't have any intentionality and understanding of the world and work automatically, they work very quickly, no data are forgotten, and only a few people have access to the results of their processing. In the era before the information society, breaches of personality and harms to it happened, but in a much smaller extent. Nowadays, the extent is much bigger and the change in quantity changes the quality to use Hegel's words. Let's go through the modern technologies to assess their risks for privacy.

Klitou (2014) considers all ICTs as privacy-invading technologies as they collect and manipulate information which can have the form of privacy information. All technologies that enhance or replace human senses are dangerous in relation to privacy. Other types of technologies like DNA analysis systems, neurotechnology,

mass surveillance technologies, etc. pose a threat too. The developing area of virtual reality supplies its provider with an enormous amount of private data on everything the person does in it including data from the body sensors. Augmented reality is not better in this context.

Klitou (2014, p. 175) characterizes current society as "increasing mobility, ubiquity, traceability, identifiability and heterogeneity/diversity of the inter-connected components of the information/digital society, and the growing enterprise for achieving unlimited storage space, bandwidth and Internet access points."

It is difficult to escape the privacy-invading technologies as they have become natural components of our lives. Without them, individuals would be excluded from society and would have a difficult life as most services have adapted to the easy use of technologies. They can make our lives easier and more comfortable releasing from annoying activities.

Privacy-Invading Technologies

Privacy-invading technologies include, according to Klitou (2014), DNA analysis systems, neurotechnology, identification technologies, nanotechnologies, advanced imaging technologies and mass surveillance technologies, open source information, data mining intelligent software, cookies, fusion centers, electronic voting machines, automatic license plate recognition systems, intelligent transportation systems, unmanned aerial vehicles or drones, ultrathin, high-resolution cameras, Google's digital services (e.g., Google Voice, Google Street View, etc.), LEXID, Facebook (and other online social networking services), cloud computing services, automobile black boxes, Deep Packet Inspection software or behavioral advertising technology (e.g., Phorm), laptop/PC web-cams, nanoelectronics, software agents/artificial intelligence, and neurotechnologies.

Considering the tracing capabilities of mobile phones, RFID technology, CCTV cameras using face recognition and biometric identification anonymity may become a utopia. The spreading of internet of things which uses a lot of information from various sensors is another potentially harmful system. Threats to privacy are not limited to public spaces; they are present in private spaces like homes as well.

Neurotechnology means technologies that can determine or intervene in the neural functioning of human mind (Klitou 2014, p. 60). An example may be the hypersonic sound which can be used to infiltrate in a particular brain exclusively. There is also an Emotiv's brain-computer interface that can read and interpret to some degree human thoughts and emotions.

Unmanned aerial vehicles (drones) are often used for surveillance or air assaults. They are often equipped with imaging systems or cameras to provide visual surveillance from the air. Images or videos are transmitted in real time. Some have thin lens-free high-resolution cameras, especially those developed by the Defense Research Projects Agency (DARPA). The amount of data modern drones developed by DARPA provide make it difficult to interpret them. High-performance software is

used to automatically analyze the data and look for specific actions and patterns of behavior.

DNA analysis allows to reveal DNA profiles which has the format of a numeric code. The profiles can be used to reveal hereditary characteristics and identify relatives. The analysis of a DNA sample can reveal information on physical characteristics, health state, and general information on the behavior. The DNA samples are left behind very easily and so they can be obtained without notice. Genetic surveillance is a real threat. The only obstacle to its massive use presents the costs of DNA analysis. Insurance companies, employers, governments are surely interested in deep analysis of the DNA.

Automatic face or object recognition like the license plate recognition poses another threat to privacy. They can be used for beneficial purposes, e.g., to search for wanted criminals or stolen objects, but on the other hand they can be used for privacy harming purposes as well.

Body scanners allow to see the naked body beneath the closing (Klitou 2014, p. 72). There is no physical contact, but the naked body is seen instead. Atoms with higher atomic numbers like metals absorb X-rays, atoms with low atomic number scatter X-rays. Human tissues have relatively low atomic number. Backscatter body scanners project low-radiation X-rays and the reflected X-rays are then detected, identified, and converted into an image on the monitor (Klitou, p. 74). Scanners can improve the screening process at airports and facilitate the workers there to detect dangerous objects. On the other hand, they are not fool proof and not all dangerous objects or substances can be discovered by them.

CCTV

Closed-circuit television (CCTV) cameras can use pan or tilt or zoom, can be remotely accessed and controlled, and can record a huge amount of high-resolution data. The data can be transmitted over the internet and easily made available (Klitou 2014, p. 115). The cameras can be further equipped with object or biometric recognition systems to rapidly identify objects and individuals including their behavior. They can have sensitive omnidirectional microphones, loudspeakers for communication of the operator with people, RFID readers, data mining software, body heat sensors, etc. They are becoming more affordable which means almost any individual can intrude upon privacy of other people. The metaphor of the Big Brother becomes supplemented with the metaphor of small brothers. CCTV cameras equipped with other devices resemble the telescreens known from Orwell's roman *Nineteen Eighty-Four*. It is not necessary that the CCTV cameras would be used to monitor people; their only presence makes people careful and changes their behavior. The self-censorship can be more powerful than exercising external control. Reminding people through loudspeakers that they are watched would intensify their self-control. Phone calls can be monitored, emails controlled, instant messaging as well, and even face to face conversations can be with the ubiquitous devices eavesdropped easily. Microphones and cameras are very small and highly effective. People are not used to this kind of threat and even when they know, they could be monitored in the public space they discuss private affairs and personal issues.

Another intrusion on someone's privacy represent the loudspeakers. They can be used to communicate orders or instructions. That can have humiliating effects on people in public and could be an instrument of social control. The CCTV cameras are favored as they can be used to prevent vandalizing of property, to lead to safer and cleaner public areas, but once they are accepted, they could be used for various reasons including social control. From this perspective, CCTV with loudspeakers could harm everyday life of people and deprive them of the right to be left alone. Cameras with loudspeakers could be used to greet customers, recommend them products or services on personal bases as they could recognize faces and buying habits, they could monitor employees and convey them commands individually, they could monitor students at schools and force them to follow the rules. The operator is separated from the persons to whom he communicates and has better information, safer situation, and more freedom than the monitored. Their relationship is no way equal.

Loudspeakers can warn potential criminals and remind them they are being watched. They can be used to discourage them from illegal activities before they start or shortly after their outbreaks. To maintain the power and respect of voice commands through loudspeakers, their instructions must be enforced if people don't respect them.

Microphones increase the accuracy of monitoring as sound is not dependent on sufficient light and wide view, is omnidirectional and because violence often starts with verbal aggression, sound allows early reactions and operations (Klitou 2014).

In any case, we must realize there are alternatives to such detailed monitoring. Klitou (2014) mentions some of them: sensors detecting dangerous substances and locating them automatic warning systems detecting unauthorized trespassers, automatic light emitting illuminators activated by an intruder, making places unattractive for the unwanted social group through music, decoration, etc., or using other methods of crime prevention like education or policemen supervision.

RFID and GPS

RFID allows identification and tracking of objects and animals and if implanted into human bodies, it would allow person identification as well. RFID is an automatic identification technology which can identify things and collect data about them (Klitou 2014, p. 160). An RFID microchip consists of an antenna, microchip, and memory. Its size ranges from a millimeter to several centimeters. The sensors can be active – powered by a battery and constantly transmitting data – or passive – activated by radio-frequency signal from RFID devices. If implanted into human bodies, they can also provide medical information.

RFID tags can be placed on almost everything people buy including clothes, jewelry, etc. Data about the consumer obtained from the credit card can be linked to it and we get personally identifiable information.

GPS (Global Positioning System) is a US space-based Global Navigation Satellite System (GNSS) that provides reliable positioning services (Klitou 2014, p. 162). A European alternative to GPS is the Galileo system. GPS consists of three parts: satellites on the Earth orbit, monitoring stations on Earth, and GPS receivers. Its accuracy is about 15 m. If combined with cell phones, it can be used for navigation purposes and for location of persons in emergencies, but it also provides private data

on location of persons. Location data can be stored and further analyzed to reveal the subject's movement.

If GPS and RFID systems are combined, the subject's movement, both outside and inside, would be monitored. RFID readers would also enhance the capabilities of CCTV systems. Obtained information could include information on where somebody lives or works, on his daily habits and movements, actual physical location, personal affairs, etc. Such information would be interesting for insurance companies, retailers, marketers, employers, etc. to analyze the person's behavior and potentially to determine or predict his future activities. The information could also be used to discriminate against some people or social groups. Moreover, monitoring people could have a chilling effect on them which would further limit their freedom. Tracking people and their movement could reveal who they meet and what they do. Undesirable activities could thus be easily discovered. People may lose any refuge resulting in nowhere to hide situation.

In the era of internet of things, the tracking potential increases enormously using information from the products. Specific locations could have their global location number which could lead to the rise of internet of places. Internet of places means that place-specific information is available to people or devices (see Cooper and James 2009). Object could contain information on their location and identification and could be identifiable in space and time.

A big issue are software viruses which could change the behavior of devices and provide attackers with private information. That can't be predictable or expectable. The problem consists also in the fact that the leakage of data may happen unnoticed.

Facebook

Facebook is a social network very popular among the European and American population. It has among 1,590,000,000 users (Statista 2016). That is why it is also a very popular marketing channel. Not only individuals but also companies have profiles on Facebook. As it is so often used, companies use it for marketing purposes. Especially companies operating on B2C markets use it very often. Companies can not only approach their customers and select those which are potentially interested in their products, but can influence their opinions as well. That is why companies cooperate with marketing agencies to make their campaign effective. Facebook advertising can be better targeted, better planned, evaluated, and tested. Facebook users can be influenced to move from Facebook on another – e.g., company – website, to interact with a picture (commenting, liking), to watch a video, to get new fans, to install an application, etc. In order to target marketing activities, Facebook analyses information inserted by its users. Facebook users insert many data when they register and other data and information when they use it. Facebook then analyses any file or information entered into it to identify and segment its users. Marketing can be targeted according to age, geographic information, interests, similar users (lookalike) according to similar traits, custom audience, fans of a certain page, etc.

When registering with Facebook, the user agrees to its terms and conditions including handling of the private information. Careful setting of the application and not entering sensitive information may reduce the dangers of privacy breaching. Some users install advertisement-blocking software which reduces the consequences of misusing personal data.

Big Data

According to Frost and Sullivan (2015), 90% of existing data have been created in the last 2 years and from 2025, the year's production of data should exceed 100 Zettabytes. Gartner defines big data as "high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization" (Gartner 2015). The volumes achieve Terabytes, Petabytes, etc. Examples of high-volume data may be user-created content, data from the stock market, etc. Velocity concerns velocity of the data flow. The data are very often unstructured and that is why preprocessing is very important. The data needn't be authentic, correct, and valuable. According to Meyers (2014), big data are used by banks and insurance companies, producers of electronic devices, and telecommunication companies. Big data are from 48% used above all for the analysis of customers and their behavior. That may be helpful and may lead to the discovery of new relations and information (e.g., in health care or marketing) and thus contribute to the development of knowledge economy. However, the problem of big data consists in the fact that new patterns and information may be found which can't be deduced from separated data, the results may be imprecise which may harm the analyzed subject, people may feel insecure, lose their private spheres, and the development of their identity may be harmed.

Phishing

Phishing misuses the complexity of current technological cyberworld and attempts to acquire sensitive often private information (usernames, passwords, etc.) by passing off as a trustworthy entity. It uses both psychological and technical methods. Phishing is an example of social engineering which involves methods of psychological manipulation with the aim to make people divulge confidential information.

Surveillance on the Internet

Internet users are not anonymous. One of the basic ways how to identify internet users is the IP address of their devices which is simply an assigned number. For that reason, this method is primarily used for device identification and secondarily for the users' identification. IP address in its version 4 doesn't offer unique address for every device as the number of IP addresses is not sufficient. New IP version 6 supplies sufficient number of addresses and every device can have its unique number and be connected with a user.

Many modern webpages save cookies on visitor's device. Cookies are small text files used for the webpage visitor identification. They store information on webpage settings, registration details, time spent on the webpage, but also private information

like basket content, etc. There are two main types of cookies: temporary session cookies deleted shortly after session closure and persistent cookies. An alternative to cookies which can be refused are web beacons – objects on webpages or emails that track users' behavior, e.g., if he has accessed some content.

Extra tracking options offer computer tracking systems like XKeyscore or PRISM which were revealed by E. Snowden. These systems monitor and analyze data on the internet and allow surveillance (Nakashima and Horwitz 2013; Ball 2013).

Virtual Reality

Virtual reality is a computer technology that replicates or creates new (imagined, simulated) environment, simulates user's physical presence, and allows for interaction. Virtual reality includes sensory experience. Modern virtual realities use headsets, gloves, and suit to provide also tactile experience. Augmented reality means augmentation of real-world environment by computer-generated sensory inputs like video, sound, etc. To make the experience realistic, the devices need a lot of data from the user and can easily monitor his behavior in the virtual environment. That poses big threats to privacy.

Cyberstalking

Cyberstalking is the use of the internet or other electronic means to stalk or harass an individual, a group, or an organization. It is motivated by an attempt to control, intimidate, or influence a person (Petinary 2001). The intruder violates one's privacy. In the cyberworld, the offender can utilize increased anonymity, independence on place, complicated protection, quick spreading, and availability of information on victims.

Respect for Privacy as an Aspect of the Quality of Democracy

Campbell et al. (2015) suggested a quadruple helix structure of four basic dimensions for the evaluation of the quality of democracy in a specific state. The model consists of freedom, equality, control, and sustainable development. Privacy is a subsidiary concept of the first three dimensions. Respect for privacy is an important aspect of freedom. Freedom from surveillance and interference into private matters reflects respect for the individual and is important for the participation of individuals on social life. Privacy manifests itself in the standard of equality as well as everybody should be provided approximately equal amount of privacy. The exceptions should be well explained and should correspond to the democratic principles. Lack of privacy reveals undemocratic control of one subject over another and lack of democratic control, which should prevent such an intrusion into private issues.

Privacy and respect for it is so one of the constituents of every democracy. It supports autonomy, public life, creativity, openness to others, courage, political discussions, and decision-making. Using the potential of ICTs against privacy would mean to hinder democratic functioning and support totality.

Metaphors for Privacy Harms

The uncertain character of today's technological world can be metaphorically compared either to Orwell's novel *Nineteen Eighty-Four* (1949) or to Kafka's novels like *The Trial* (1998) or to Huxley's *Brave New World* (1932). Either people would lose privacy against their will in a world governed by someone; or the world becomes very nontransparent and people won't understand it any more, the processes would be too complex and complicated and nobody would understand to which purpose they serve, people wouldn't be sure if they have privacy or not; or people can surrender privacy voluntarily in exchange for other goods or because they wouldn't understand its relevance any more in the world of entertainment and easy life.

These dystopian metaphors present deterrent examples of lacks of privacy, but don't contain instructions on how much privacy in what context is advisable. We can just learn from the more or less general perspective and examples and define our ideal privacy definition.

Solove in his article (2001) uses the two above-mentioned metaphorical dystopian descriptions of current situation in information privacy. The first one is the well-known Orwell's depiction of Big Brother in his novel *Nineteen Eighty-Four*. It consists in the role of government which monitors and regulates every aspect of its citizens' life. "Big Brother is watching you" is the famous phrase that summarizes the reality in the Orwell's Oceania. The state controls, governs, and constructs everything including language; it rewrites history and indoctrinates the population. Goal of the government is uniformity, discipline, and order, privacy is in this goal's way and must be abolished, i.e., made public and controlled as a means of controlling one's individuality. Surveillance, monitoring, and spying are the predominant methods of governing. Citizens never know when they are being watched which changes their behavior. The Orwell's metaphor understands domination over privacy in terms of power (Solove 2001, p. 1415).

Solove recognizes usefulness of this metaphor, but points to its limits as well. Monitoring and surveillance is important in the control of individuals, but today information and databases are used for different purposes. Marketers use information to observe behavior in order to tailor goods and services to individual preferences. Power is not their main instrument; they rather use manipulation. They study and exploit individuality. Their goal is not uniformity and conformity, but exploitation. Information that is collected on internet users is relatively innocent, it doesn't concern pornography, terrorism, etc., but rather hobbies, financial transactions, purchases, etc.

To capture the second aspect of information use, Solove applies Kafka's metaphor from his novel *The Trial*. The main character doesn't understand why he has been placed under arrest. He tries to find out why he has been arrested, but can't find anything clear. Everything is secret and mysterious, he finds fragments only. The authorities are inaccessible to him. As Solove puts it: "Kafka depicts an indifferent bureaucracy, where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process. This lack of control allows *The Trial* to completely take over Joseph K.'s life. *The Trial* captures the sense of helplessness,

frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life" (Solove 2001, p. 1421). Joseph K. can't fight back, doesn't know what the authorities know about him, how his data have been processed. He is powerless. In the information society, processes are efficient, standardized, and cultivated and lead to bureaucratic organization in Weber's sense. All emotional and accidental elements are eliminated. Power in *The Trial* has no goal, it just works effectively and nobody can understand it. People without control over their personal life and personal information become very vulnerable and weak. Current emphasis on quantifiable data which can be processed has social effects and changes the way people are treated and understood.

There is, however, one more metaphor which supplements the perspective on privacy. Solove mentions it, but subsumes it under the Big Bother category. It is the Huxley's *Brave New World* dystopia. Power used in Huxley's novel is not prohibitive and aggressive, but pleasant and entertaining. People are enslaved voluntarily. Government uses propaganda, conditioning, and indoctrination. In Huxley's book, there is a government ruling over the society and taking measures to govern it. For the entertaining type of totality, there needn't be a dictator as citizens become addicted and require the impression of easy life themselves. This type of totality is not even considered unfree. According to Postman (1985), Huxley feared there would be no reason to ban books as there would be no one willing to read them, people would have so many options and information that they would be reduced to passivity and egotism, there would be so much information and communication that people wouldn't be able to grasp it and truth would become irrelevant, everything would be easy and trivial. Man's infinite appetite for distractions was underestimated in Postman's view. Too much stressing of man' individuality and disrespect of anything else may lead to this conclusion as entertainment is for man more pleasant than more valuable activities. Horkheimer and Adorno (2002) also stress the concealing character of entertainment that relieves the burden of shallow life without deeper sense.

The three dystopias depict three ways how people may lose privacy. Either by force, or without notice of the loss, only the consequences would be felt, or voluntarily in exchange for easy entertaining life.

To avoid both harms and dystopian visions, we need conscious human beings respecting and appreciating privacy. Everybody should have the right to determine his level of privacy within some social limits. The limits reflect a common cultural background. At the end of our commentated overview, we will summarize the main features of the European and American legal regulation of privacy. They also reflect the relevance of the content of privacy different in different cultural backgrounds.

Legal Regulation of Privacy in EU and USA

History and Development of Privacy Protection

In the 1970s, the US Advisory Committee on Automated Personal Data Systems and the Privacy Protection Study Commission issued in response to the use of computer systems containing personal information some reports. In 1980, the Council of

Europe adopted a Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. At the same time, the Organisation for Economic Cooperation and Development (OECD) proposed similar privacy guidelines in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The US Federal Trade Commission paid attention to the privacy issues since 1995 and 1998 published a report (Pitofsky et al. 1998) which included the Fair Information Practice Principles of Notice, Choice, Access, and Security. In 2013, the OECD issued revised guidelines in a document with the name OECD Privacy Framework (2013).

The first statutory implementation of Fair Information Principles (FIPs) in the world was the Privacy Act of 1974 which applies FIPs to federal agencies in the United States. In 1995, the EU adopted Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the personal data. In 2016, the EU adopted the General Data Protection Directive which suggests an index and restatement of most FIP principles in Article 5 (Gelman 2016).

Many organizations issue specific regulations containing incomplete versions of FIPs. In a report from 1998 (Pitofsky et al. 1998), the Federal Trade Commission identified the five principles of privacy protection: Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security; and Enforcement/Redress.

From 1998 to 2010, the FTC published various not always consistent versions of FIP principles. In 2012, The Federal Trade Commission issued a major report about privacy (FTC 2012). The text includes three main principles: Privacy by Design, Simplified Choice for Businesses and Consumers, Greater Transparency.

Current Situation in Privacy Regulation in EU and USA

In the EU, the Data Protection Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) adopted in 1995 regulates the processing of personal data within the EU. In May 2018, it will be superseded by the General Data Protection Regulation, which was adopted in April 2016.

According to the Directive 95/46/EC, personal data should not be processed at all, except when conditions falling into the categories of transparency, legitimate purpose, and proportionality are met. As for transparency, data may be processed only if at least one of the following is true (art. 7):

- when the data subject has given his consent
- when the processing is necessary for the performance of or the entering into a contract
- when processing is necessary for compliance with a legal obligation
- when processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed

- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject

The data subject has the right to access all data processed about him. The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules (art. 12).

The processing must have a legitimate purpose, i.e., personal data can only be processed for specified explicit and legitimate purposes and may not be processed further in a way incompatible with those purposes (art. 6b).

According to the Proportionality Principle Personal data may be processed only insofar as it is adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed. The data must be accurate and, where necessary, kept up to date; The data shouldn't be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed (art. 6).

The new regulation called General Data Protection Regulation (Regulation (EU) 2016/679) has broader scope than the previous directive and will also apply to data processors and controllers outside the EU if their activities relate to EU citizens. Additional obligations for data controllers and processors will be introduced. Companies will have to implement privacy and security policies and in case of data breach, competent supervisory authority will have to be informed. Consent is specified as freely given, specific, informed, and unambiguous. Data controllers must provide individuals with information on processing of their personal data. It won't be allowed to transfer data outside EU if adequate level of data protection is not guaranteed. Generally, the rights of individuals will be strengthened (Hunton and Williams 2016).

Compared to the EU, USA don't have one privacy protection law. In general terms, privacy is in the USA interpreted as the right to be left alone and is based on the protection by the Fourth Amendment right to be free of unwarranted search or seizure, the First Amendment right to free assembly, and the Fourteenth Amendment due process right. The USA prefers the sectoral approach where certain sectors (e.g., media, Health Care, Banking) are regulated by a mixture of law and self-regulation.

The EU law is more complex and specific than the US law. Some concepts are similar, but most of the EU data protection guarantees simply do not exist in US law. In the EU, the expectation and reliance on privacy is stronger than in the USA. EU law covers all persons regardless of their domicile or address, US law distinguishes between US and non-US persons (Boehm 2015).

Conclusion

Man needs privacy not only for the development of his autonomy, but also for the development of social relations which are private by its essence and are determined for the participating individuals only. The development of technologies in current

cybersociety provides man with many simplifications and comforts including knowledge distribution and its utilization in knowledge economy and knowledge society. However, the reversed side of these benefits consists in creation of new environment which man doesn't properly understand and doesn't control. The technological devices and instruments require a lot of information on their users to provide their benefits. People supply them with private data and don't notice the threats and harms to privacy related to that. That is a problem because people will be affected by these consequences anyway and should know them in advance. In future, we can expect development of more sophisticated devices with advanced functioning and privacy will be even more endangered. Internet of things, industry 4.0, autonomous cars, drones are just a few examples of new trends which will require, store, and process big amounts of data many of which can be sensitive.

In order to take full advantage of the benefits offered by the knowledge economy and knowledge democracy, we need to avoid the risks related to the privacy information misuse. For that, men should be educated on risks of privacy invading technologies and should learn and develop all three types of human activities as they were distinguished by H. Arendt (1958). That is a precondition for the proper development of knowledge democracy and full development of human potential. Arendt distinguishes between labor, work, and action. Labor is the production of things for the consumption and satisfaction of human needs. Work consists in the production of durable things like artworks. Action is the revealing of oneself to others in speech and action in the politic realm. Even though these activities are in reality not separated, they can be distinguished and appreciated methodologically.

But the situation is not so simple. We haven't found any precise definition of privacy; there are only structural definitions available. The concrete definition of privacy must be found in relation to specific context only which includes culture, involved persons, motivation, etc. We can learn from previous experiences including the dystopian visions, try to find a common defensible concept of privacy, but without claim to any final solution. Here also lies the role of knowledge democracy where people can learn from one another, discuss and develop their opinions, and fight for their interests.

The new cyberworld offers new ways of privacy protection, but also new privacy threats which are not counterbalanced by privacy protections. Even though we can't understand and predict them all, we can think of them and discuss them. And that is the role of ethical thinking. The technology can't save us, only its ethically responsible use respecting human dignity including privacy can. For that, the knowledge democracy is a suitable environment.

References

Arendt, H. (1958). *The human condition*. Chicago: University of Chicago Press.

Ball, J. (2013). NSA's Prism surveillance program: How it works and what it can do. theguardian. http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google. Accessed 12 Nov 2014.

Boehm, F. (2015). A comparison between US and EU data protection legislation for law enforcement purposes. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf. Accessed 26 June 2016.

Campbell, D. F. J., Carayannis, E. G., & Rehman, S. S. (2015). Quadruple helix structures of quality of democracy in innovation systems: The USA, OECD countries, and EU member countries in global comparison. *Journal of the Knowledge Economy, 6*(3), 467–493. https://doi.org/10.1007/s13132-015-0246-7.

Cohen, J. E. (2012). What privacy is for. *Harvard Law Review, 126*, 1904–1933.

Cooper, J., & James, A. (2009). Challenges for database management in the internet of things. *IETE Technical Review, 26*(5), 320–328.

Descheemaeker, E. (2015). The harms of privacy. Edinburgh School of Law research paper no. 2015/27. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2644285. Accessed 21 June 2016.

Federal Trade Commission (FTC). (2012). Protecting consumer privacy in an Era of Rapid change: Recommendations for business and policymakers. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. Accessed 26 June 2016.

Floridi, L. (2005). The ontological interpretation of informational privacy. *Ethics and Information Technology, 7*(4), 185–200.

Frost & Sullivan. (2015). World's top global mega trends to 2025 and implications to business, society and cultures. http://www.investinbsr.com/ipaforum/wp-content/uploads/Iain-Jawad-IPA-Forum-2014-Presentation.pdf. Accessed 18 Dec 2015.

Gartner. (2015). http://www.gartner.com/it-glossary/big-data. Accessed 18 Dec 2015.

Gavison, R. (1980). Privacy and the limits of law. In F. D. Schoeman (Ed.), *Philosophical dimensions of privacy* (pp. 346–402). Cambridge: Cambridge University Press.

Gelman, R. 2016. Fair information practices: A basic history. http://bobgellman.com/rg-docs/rg-FIPShistory.pdf. Accessed 26 June 2016.

Harper, D. (2001). Online etymology dictionary. http://www.etymonline.com/index.php?term=private&allowed_in_frame=0. Accessed 20 June 2016.

Horkheimer, M., & Adorno, T. W. (2002). *The dialectic of enlightenment*. Stanford: Stanford University Press.

Hunton & Williams. (2016). EU general data protection regulation finally adopted. https://www.huntonprivacyblog.com/2016/04/14/eu-general-data-protection-regulation-finally-adopted/. Accessed 26 June 2016.

Huxley, A. (1932). *Brave new world*. New York: Harper & Brothers.

Kafka, F. (1998). *The trial*. New York: Schocken Books.

Klitou, D. (2014). *Privacy-invading technologies and privacy by design*. Hague: T.M.C. Asser Press.

Meyers, D. (2014). Big data: A competitive weapon for the enterprise. VizWorld. http://www.vizworld.com/2014/12/big-data-a-competitive-weapon-for-the-enterprise-infographic/. Accessed 18 Dec 2015.

Moor, J. H. (1990). The ethics of privacy protection. *Library Trends, 39*(1), 69–82.

Nakashima, E., & Horwitz, S. (2013). Newly declassified documents on phone records program released. *The Washington Post.* July 31 2013. https://www.washingtonpost.com/world/national-security/governments-secret-order-to-verizon-to-be-unveiled-at-senate-hearing/2013/07/31/233fdd3a-f9cf-11e2-a369-d1954abcb7e3_story.html. Accessed 12 Nov 2014.

OECD. (2013). The OECD privacy framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 25 June 2016.

Orwell, G. (1949). *Nineteen eighty-four*. New York: Harcourt, Brace & Co.

Petinary, D. (2001). Cyberstalking investigation and prevention. Computer Crime Research Center. http://www.crime-research.org/library/Cyberstalking.htm. Accessed 12 June 2016.

Pitofsky, R., Azcuenaga, M. L., Anthon, S. F., Thompson, M. W., & Swindle, O. (1998). Privacy online: A report to Congress, Federal Trade Commission June 1998. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf. Accessed 12 June 2016.

Postman, N. (1985). *Amusing ourselves to death: Public discourse in the age of show business*. New York: Penguin.
Rössler, B. (2004). *The value of privacy*. Cambridge: Polity.
Sennet, R. (1977). *The fall of public man*. New York: Knopf.
Solove, D. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53*(6), 1393–1462.
Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560.
Statista. (2016). Leading social networks worldwide as of April 2016. http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. Accessed 21 June 2016.
Van de Hoven, J. (2001). Privacy and the varieties of informational wrongdoing. In R. A. Spinello & H. T. Tavani (Eds.), *Readings in cyber ethics* (pp. 488–500). Sudbury: Jones and Bartlett Publishers.

Cyber-Challenges and NATO

44

Marios Panagiotis Efthymiopoulos

Contents

Abstract

This chapter argues for a global strategic framework of operational capacity and resilience in the field of cyber-security reflected toward NATO's current and future policies on security resilience. The chapters examines and discusses interoperability of aims and objectives in cyber-security as a global necessity so we may define law, rules and regulations, policy attributions, and authorities. It analyzes possible structures that are needed to be put in place on a global scale to defend

M. P. Efthymiopoulos (✉)
School of Law, University of Central Lancashire (UCLan Cyprus), Larnaka, Cyprus

Strategy International, Larnaka, Cyprus

Strategy International, Thessaloniki, Greece
e-mail: MEfthymiopoulos@uclan.ac.uk; marios.efthymiopoulos@strategyinternational.org

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_47

security structures and members of the Alliance, reflecting issues of cyber-security. The chapter aims to define current threats and future challenges. Cyber-attacks are elements of asymmetrical or hybrid threats. The future of e-safety lays at the global estimation of cooperation against specified or approximate threats.

Keywords
Cyber-security · NATO · Resilience · Interoperability · Alliance · Strategy · Cyber-defense

Introduction

Cyber-security is a framework policy of defense and protection. It is adopted as central policy command by the State and Government allies but also private institutions/organizations.

Cyber-security is an institutional policy for NATO in 2018. It reflects elements of security and safety in the virtual world of the Internet. It is a procedure. It follows the rule that both individuals and collectives should be protected from malware attacks. Security and safety include hardware and software protection.

When cyber-security is assessed from the point of view of the discipline and sciences of security studies and political affairs, cyber-security is defined as a policy framework, a methodology, and an orientation and application for all matters relative to the world of the Internet when interconnected.

Cyber-security, as a discipline of interdisciplinary science, defines the government and countries' strategic approach on defense through technological development. Elements and variables of safety and defense are examined. Policies relate with the county's protection in infrastructure, organizations, and businesses located and based in the country(ies). Government policies relate also to the individual, the citizen, and/or resident but also collectives.

Cyber-security as a policy of security resilience reaches out for technological agility. It is a policy approach that reflects growth and sustainable development. Cyber-security is a method of protectionism; defending method and policy against e-threats and attacks; protects critical infrastructure and private infrastructure; its defend method and actions include the protection of both software and hardware. Necessary to achieve such a goal is to have a wired access point to the World Wide Web, (AKA, the Internet).

Research and development (R&D) in 2018, methods in the fields of cyber-security, ensures resilience and security in the field of technology and cyber-science. Cyber-security is being built not only as an option against malicious attacks among others but also in essence allows for technological growth and advancement through research and development methodology (R&D) through and among which we may achieve *optimum capacity*, *adaptability*, *and affordability of technology in both infrastructural and private levels.*

Resilience is a strategic objective in security studies. It is an element of political and business continuity that provides for strong will to continue meeting strategic goals, when objectives, missions, and vision have been proclaimed. When reflecting

resilience in cyber-security, the evolution of strategic and operational capacity is displayed, in which it safeguards and enhances methods and tools of protection against malicious attacks.

National security and defense strategies rely on cyber-security protection policies and application methods, how cooperation can and will be achieved, and information agility and technological advance mechanisms, considering the multidimensional level of threats and challenges.

Cyber-security is yet to be strategically defined at a global scale. It needs to be defined, legally and politically at a global scale, through appropriate laws, through global organizations such as the UN. A policy regulation should govern rules and policies, definitions, and actions.

This chapter argues and requests for a global strategic framework for operational capacity and resilience in the field of cyber-security. This chapter examines the necessity for interoperability on cyber-aims and objectives against possible threats and challenges, without which no universal law can be created or implemented. Cyber-attacks are elements of asymmetrical or hybrid threats. The future of e-safety lays at the global estimation of cooperation against specified or approximate threats.

Operationally, national and cooperative forces need to be continuously agile and technologically advanced. In an asymmetrical world, which is complete with unforeseen challenges and threats, we need forces with flexibility, adaptability, and operational and strategic command structure, based on high technologically sophisticated information "coming in" but also being used while in training or through active operations.

On a theoretical scale, the current chapter requests cyber-security strategic framework adoption of a resilience and adaptability and interoperability policy in the framework of safety and defense. Theory may create policy for cyber-resilience against hybrid threats. It will testify for a new approach on aspects of cyber issues.

The current chapter reflects an interdisciplinary approach and combines elements of global security and strategy, national and international law, economic development, and technological research and advancement.

Its creation is a result of a set of primary experiences and acquired sources of information, interviews, travels, and exchange of expert opinions through governmental and private institutions. The joined work and experiences gained shaped the understanding and need to request for a specific resilient and global policy in the framework of cyber-security. Arguments and statements of the author are put forward, reflecting both current but also future threats on cyber-security-related subjects.

The chapter will frame the policy necessity of creating a grand cyber-security strategy for the twenty-first century. It will define the "dynamism" of cyber-security both as a topic and subject. Cyber-security is a twenty-first century element of policy orientation, a necessity for collective defense and resilience of each nation's protection of infrastructure and the individual.

A grand cyber-security strategy will allow for the creation and unfolding of a complete new world, set with standards, policy procedures, and recommendations, surely differentiated from the "analogic world." A strategy of cyber-security will unfold options and opportunities: a technological advancement and dynamism of

innovation and sustainable futuristic advancement. It will further progress the necessity and importance of the Internet in a form that is limitless. Resilience and interoperability in cyber-security will also unfold. A policy of a joined cyber-security strategy will combine knowledge efficacy, construction, production, and application through protective and defensive measures applied.

Considering the strategic needs for cyber-resilience, the chapter will outline the necessity of a joined strategic positioning of the willing. It proposes a tactical and operational military and civilian capacity-building approach, based on global scale standards, relatively similar to Alliance standardization and preparedness agreements. It is a smart-leveled security policy orientation. It will benefit those that seek peaceful cooperation in a digitized and interconnected world. It applies for those that seek a balanced relationship.

With this current chapter, we examine and evaluate strategic information; we assess current knowledge; we propose options for an "ecumenical scale leveled cyber-security and defense policy strategy," with which combined with a universal legal regulation on cyber-security and cyber-defence. The chapter clarifies methods, rules, and policies; reflects on the current and future period of technological agility and cyber-advancement; the chapter examines possible methods foresighting or predicting future requirements in the need for defense of each nation's national critical infrastructure, individually or collectively as allies.

This is an important subject of research that currently is being updated through new information and experience. A recent research-based evaluation on an alliance of nations was put forward bringing NATO's cyber-resilience specialization as a necessity in the framework of a possible creation of a global-scale grand strategy on cyber-security (Efthymiopulos 2013). Considering the earlier outcomes of the research, in effect we add more value to the necessity of strong allies through institutional alignment, in operational security and defense capabilities.

The issues presented, henceforth, are for consideration and examination, adding value to the researcher, the professional reader, and the decision-makers that seek solutions for a strong viable alliance strategy in cyber-security.

Resilience

Resilience as a terminological and operational factor is a brand name with operational capacity to sustain and grow. Resilience adds value to an already robust policy decision and operational capacity building and actions, a "stronghold" for cyber-security policies.

Resilience's framework acknowledges the policy of preparedness as an integrative part of possible emerging crises. It is seen as a strategic management policy procedure and tool. Strategically, it applies to operational capacity building, both civil and military and as aforementioned is an element of acknowledged standardization of procedures.

When forces are for deployment, a more flexible and effective means of countering threats, it will be adaptable to mitigation and/or negotiation procedures with

non-NATO members and will allow for cooperative members' joined cooperation and training, in consequence, to relative past or currently emerging challenges and threats (i.e., NATO-Russian relations and NATO-ICI members considering the threat of ISIS and other terror groups).

NATO's resilience will redefine strategic plans and reassess risks. Heads of state and governments at NATO should create a "modern administrative and operational format of the alliance" that is flexible and e-oriented. NATO truly needs to hold agile and technologically advanced forces with added value through civilian capabilities and social media training and action, among others.

Resilience therefore should become also an adaptation process for NATO, a phase to consequently strategize and draw new scenarios. This is in order to operationally process and counter in an effective manner current, new, and upcoming challenges and threats. Resilience is therefore a policy that is being given way from "NATO's Smart Defense" clause. A result and constant request of NATO is to boost change if it wants to remain relevant and most importantly a global asset value to security and strategy.

The policy of "resilience" should open way to operational and strategic flexibility. It will be applied at all levels. When strategically managed and operationally approved, resilience will include a further and concrete development of an "updated" cyber-defense policy for NATO among other policies that will add value to the needs of NATO to counter threats in a multidimensional level.

NATO's Smart Defense should be resilient. It should ensure stability. The Atlantic Council of the USA refers to a "stability generation" policy (Kramer et al. 2016), adding that NATO's collective defense itself should be re-strategized. It should be adaptable to the constantly increasing needs, for a technologically secure and agile environment, in a period of great challenges and threats from outside but also within NATO space.

A resilient smart defense requires agile network e-centric cyber methods. NATO requires operational capacity steps to be adopted. Through a methodological reasoning and step-by-step deployment of forces in security and e-security-led operations, NATO will be able to secure its e-space, secure its infrastructures, but also provide defense and cooperation, as NATO should "confront where we must and cooperate when we can," referring to the NATO-Russian relations, according to Stavridis, the Dean of the Fletcher School at Tufts University.

Due to the importance of a resilient policy to collective defense, cyber-defense as a policy should become a core asset value policy for the Alliance. It should be used as a core element for a renewed flexible, otherwise resilient, smart defense policy, for the benefit of collective defense but also cooperative adaptability.

NATO's Cyber-Resilient Policy

"Future war-like operations will be held in a far more complicated level of military operations" (Efthymiopoulos 2008a). Current military operational and tactical needs, considering the asymmetrical and multidimensional environment, require

good and agile capacities and capacity building. Joined forces themselves require proper command and operations. They require agility but also resilience.

We live in an age "...in which more people have access to highly sophisticated technologies and almost every social, economic or military asset has become 'securitized' or vulnerable to disruption – whether temporary or more lasting – from an outside attacker or even an inside source...In a globalized but also more confrontational and complex world, resilience will remain an ongoing concern for Allies, requiring constant adaptation as new vulnerabilities and threats emerge... (Ibid 3)."

Operations are conducted today within a complex environment. The use of technology necessitates accurate "tools" for possible success. They require interoperability of forces, in a constant adaption environment. The same applies for network-centric-oriented operations where cyber-resilience is required.

Technology is therefore used as an asset tool. Its capabilities are used for the success of military operations. Knowledge and good use of technology, and in specific cyber-defense, are added values that minimize among others' human cost.

When NATO leaders first considered cyber-security as a policy requirement, questions were raised on how to find a smart way and operational way to use technology for its benefit both operationally and strategically in a fast and technologically advancing world.

In twenty-first-century security affairs, NATO forces are required to be well prepared for possible rules of engagement at all levels and dimensions. They should be able to counter symmetrical and asymmetrical battles, threats, or challenges. At the level of cyber-resilience preparedness, scenarios, of possible attacks and battles, can be anticipated. There are or should be proposed operational methods for action whether this is for defense or cooperation.

Technology today is limitless; reflects both military and civilian assets and so is the virtual world of defense, where technology and cyber-defense merge. These are the tools for action. Technology plays a key role in a global reach and so does NATO, through the framework of a limitless technology. NATO uses technology for the preparation of its forces, as tools for knowledge as to defend but also to counter-assault, where countermeasures are needed.

Since the adoption of the NATO Cyber-Defence Policy (NATO's Cyber-Defense Policy 2011), NATO trains its military and civilian assets for possible action against possible threats. NATO is constantly training its forces on cyber-defense. Training can be achieved through national, bilateral, and even multilateral levels of NATO, through the association of member states, at the level of Centres of Excellence, such as the CCDCOE (NATO Cyber-Defence Centre for Excellence, https://www.ccdcoe.org/). Training is a necessity, while NATO gets more engaged in field cyber-network centric operations. It is anticipated within the Alliance that NATO is well prepared, both for current and future challenges, countering multiple and multileveled dimensions of cyber-attacks. Yet, it also holds an open option, if necessary, to conduct counteroffensives to prevent further escalation of cyber or military actions (Hughes 2009).

NATO missions "will continue to require agile and interoperable, well-trained and well-led military forces" (Ibid 1). This new technological and operational

environment through cyber-defense provides NATO with a new level of technological possibilities, new tools for use against possible threats but also protective "cyber-objectives." Allies have an added policy, mission, and value. Ongoing and constant transformation through its operational and capacity-building resilience aims to reach in updated capabilities and political excellence, in 2016. NATO aims for well-coordinated missions in cooperation with and/or participation with other international organizations, when prompted to react on international threats or challenges. As such, NATO has the ability to continue to be a force and security provided in future potential of, what we may call it, the "online" security protection initiative against all possibly known threats.

Now it seeks excellence in achieving the best smartest way to protect but also counter-attack. By "nature" NATO exists to prevent and defend member states from attacks.

Through smart ways and agile training, NATO can counter most known ways of interface (whether virus or virtual) attacks or spying attempts.

As previously noted, cyber-defense capabilities, in a smart and resilient way, are the "operative goal." NATO members prepare well and at joint levels. NATO's Smart Defence, a policy framework for defense tactical advice and operations, used to be the method that, among others, branded the need for a cyber-defense policy (In the following sub-chapter, I include the analysis of a research method to explain the meaning of Smart Defense. It was presented at a conference under the name of "The Shadow Summit of NATO's Washington Summit of 2012", http://www.natowatch.org/node/676 organized on May 14–15, 2012 at The Elliott School of International Affairs, The George Washington University Washington, DC. You can also see live the speech at Cspan on http://www.c-spanvideo.org/mariosefthymiopoulos.). Through a possible upcoming cyber-resilience of NATO, which could be adopted as a policy, among other resilience policies, during the Warsaw Summit in July 2016, NATO will be expected to take preliminary actions through standardized procedures of protection effectiveness. What is well known through policy analysis is that NATO military forces should reach an appropriate level so as to operate in and around "article and non-article 5 operations" (Sendmeyer 2010) – meaning not only defensive-clause operations but also in counteroffensive operations (NATO 2008a). Cyber-protection is needed when defense of allies is associated with possible threats or challenges such as the one of ISIS.

This article stresses that NATO Cyber-Defence policy should never stop transforming, while technology progresses and threats expand to a new and deeply digitized world of insecurity starting with the case with the cyber-attacks in Estonia in 2007 (Rehman 2013). Past events in Estonia, showed early on a strong smart cyber-defense "umbrella" which is certainly needed by 2016, in which agility and resilience need to be achieved.

There is a need of a resilient policy method approach for continued practical allied update and practical preparation to counter cyber-attacks. Innovative methodology and ideologies are needed to process such a policy approach.

In turn, a preparatory resilience policy applied will allow for the 28 member states to be even more agile for defense or crisis management purposes and electronic

warfare methods. Interoperability of forces for joint use in cyber-defense should be achieved through adaptability and standardization processes. NATO should "e-volve" as should Allied "e-networked" states. NATO should innovate and manage. NATO should administer change on methods of smart resilience in defense through cyber-defense, strategically and operationally.

Cyber-Resilience in Cooperative Defense

During the Chicago Summit, NATOs' policy on "Smart Defense (NATO Chicago Summit: http://www.chicagonato.org/ May 20 & 21 2012)" was presented in which ". . .NATO leaders agreed to embrace Smart Defence to ensure that the Alliance can develop, acquire and maintain the capabilities required to achieve the goals of 'NATO Forces 2020. . . (Ibid 1)." Following this, during the Wales Summit (Wales Summit 4 September 2014, http://www.nato.int/cps/en/natohq/events_112136.htm [seen May 1st 2016]), NATO Allies confirmed and reaffirmed the commitment of all member states to consider the cyber-resilience of each nation to the aims and objectives of the Alliance. They affirmed NATO's policy vis a vis the international and interconnected environment, which is complete with challenges and threats. They also affirmed the raising importance of the element of cyber-security and cyber-defense. The upcoming NATO summit in Warsaw in July 2016 is yet to show the policy or resilience and cyber-resilience in the framework of cooperative defense. At a time of much needed proposal for practical and smart defense, there is a new security culture comprehension, which is now considered as multileveled and multidimensional.

Defense capacity building for the twentieth century requires a modern way of thinking. It is about encouraging cooperative defense at the level of expected outcomes considering global but also regional risk assessments. NATO is still to enhance but also maintain military capacities and military capabilities.

The new strategic concept of NATO requests the Alliance to move forward. Twenty-first century needs and challenges require agile and compatible forces at all levels, including network-centric operations and defense.

NATO forces cannot be static. They need to technologically advance and progress methodologically to accommodate the increasing need for multidimensional ways of security and defense. NATO needs to have interoperable, capable, and well-equipped technologically agile forces.

Planning and budgeting for operations need to be "smart." Directed funds should now, at a period of specialized or tailored fiscal management, build such capacities, in which planning should be effectively applied in practice. This includes where operational viability of forces is realized, on a minimum budget level with equalized costs and enhanced technology and minimum engagement in regard to both time and operations.

Throughout the attempt to achieve a truly cooperative defense, "Smart Defence" stands out on renewing operational and tactical effectiveness, operational alliance,

and coordination. It is all about specialization of forces including the element of resilience of forces mainly through technological agility.

Smart Defence is to soon prioritize to meet the NATO Force and Command Structure of 2020, through the following steps: (1) sound strategic structuring and planning; (2) good operational coordination in exercises and in the field; (3) specialization of force structure, command, and operations; (4) achieving collective defense, through collective efforts; and (5) burden sharing (6) technological advancements, considering the threats and challenges of the twenty-first century.

By 2018, in a period of much needed strategic and tactical resilience, smart defense stands out as a request for geopolitical capability and capacity, implementation, and operational effectiveness, in both the regional and global fields, in environments which are symmetrical but also asymmetrical, with minimum cost possible, through the optimum use of technology provided. While also trying to avoid duplication of efforts, member states should hold joined operational strategic centers, on and for, among others, ballistic missile defense, intelligence, surveillance, reconnaissance, cyber-defense and security, maintenance of readiness, training, and force preparation but also agile deployment bases for effective engagement; all aforementioned should be expected to work with minimum cost, casualties, and high level of technology preparedness that are both beneficial and practical.

Smart Defence is a priority policy for NATO and so should cyber-resilience in the Alliance. Through a methodological period, NATO should continue to be able to counter current and emerging challenges. Defense planning, operations, and lessons learned are therefore a continued process of evolution of NATO's capabilities which always need to be taken into account.

Resilience through smart and cooperative defense requires NATO's cyber-defense effectiveness. It also requires decision-making and leadership in this policy context. In the framework of cyber-defense, NATO needs to align supranationalized national capability priorities and standardize through NATO processes. In the framework of cyber-resilience at NATO, policies on standing management of operations need to be agreed upon. Therefore, cooperative- and consensus-leveled agreements need to come forth; NATO should produce a cost-effective projection planning and application for all operational exercise theaters reflecting the real yet also virtual worlds.

Cyber-resilience and methodological specialization through leaders' policy decisions at the level of heads of state and government in operational planning and practically applied are key components of and for success for the Alliance, considering threat assessments. Resilience with coordinated efforts may lower costs, fiscal, administrative, and human but will require developed technology infrastructure. It will guarantee national engagement of states to NATO policies, when correctly pointed out. Let us not forget that specialization as a key national policy is and will always remain a form of national interest, which examined changing variables based on geographical interests, strategic sharing of costs, technological information, and intelligence sharing or operating in regional or global environments.

Associating Smart Defense with Cyber-Resilience: "Engagement Through Policy Adaptation"

Not many steps take have been achieved in the framework of Smart Defence capabilities when resilience is applied. The inability and/or unwillingness of member states, for political and military national engagement, has still to be confronted, mainly as fiscal austerity measures are applied and cutbacks are in effect (Chicago Council on Global Affairs 2012). According to the Atlantic Council, "...The Alliance, given the new strategic landscape it currently finds itself in, requires a new strategy. NATO's current three core tasks – collective defense, crisis management, and cooperative security – are 'tasks' but not strategies – they do not identity the full spectrum of ends, ways, and means, and therefore do not tell the Alliance and its members either what to do or the risks involved. NATO has been working diligently but without great clarity or common agreement as to its end goals (Ibid 6, pp. 3)."

Heads of state and governments however do listen and observe and therefore consult and call on NATO to hold summit meetings and to negotiate or mitigate issues such as the upcoming Warsaw Summit of July 2016. In the framework policy "Smart Defence," which is yet to be achieved by 2020, Smart Defence renders cheaper the cost for the total sharing of burden by member states while it is attracted more to elements or variables where technology is used to minimize costs. Surely, not all members share the same burden to this day, as also the cost differs from state to state and so does aforementioned national interests.

In a time of austerity measures and political challenges and changes, states are still to realize how cost can be measured in a smart "budget-and-operations" way. While Smart Defence lowers overall long-term cost, and if burden sharing is actually increased but equalled to lower levels of fiscal sharing, long-term results will show that, in fact, less cost will be achieved.

The cost will be equally associated with the value of services provided and reflect the needs of strategic management and planning of all 28 member states, which to be fair cannot yet be achieved.

While, national and collective defense remains at the forefront of interests of states, a new "rapprochement" is needed between member states as threats are now borderless.

Cyber-defense, being a key core policy for smart defense and resilience, attracts attention to stake holders. Through evolving and constant communication and marketing perspectives, social media and workshops, and conferences, cyber-defense should continue to be promoted and have a clear aim. Reflecting on the needs for a global element of cyber-security against current and emerging challenges, exchange of scientific information and operational processes promotes such ideology, where experts from around the world exchange information and discuss the risk assessments and how to manage them.

Cyber-defense, a core policy in Smart Defence itself, works as a "decree of specialization, which now requires adaptation if not done so already for each member state" politically, strategically, tactically, and operationally but also legally.

Cyber-defense policy must and should always be provided as a methodological tool for operational success of NATO against current and emerging threats. It is and will always be a tool for a joint framework of cooperation, globally.

As Smart Defence is being upgraded and developed, cyber-defense is ". . .not a conception but a real-politic issue. . . (Ibid 4)" and should remain an element of specialization policy, a key for concrete strategic engagement of all resilient member states. It will emerge to become a policy of unity among states (political) and business continuity (strategic orientation) about the future of NATO.

NATO's strategic approach post-Warsaw Summit is estimated to reflect a much need realistic plan of operations and engagement in the field of cyber-security and defense. NATO should continue to be a collective to be a force projector and force protector. It should not limit its role and actions but should allow and seek out enlarged cooperations tailored to the global and regional needs to counter the existing challenges or emerging challenges, considering that as aforementioned, challenges are now borderless.

Cyber-defense and technological progress within NATO can therefore be seen as the core of collaborative smart defense, to be finalized and achieved by 2020 standards. Cyber-security being technologically advanced is resilient to changes. It does provide adaptable technological architecture and posture which will be discussed below considering the opportunities but also challenges. For Cyber-Security to be effective, e-infrastructure is needed, limiting human capital, making the policy and installations affordable and "added value for money and secure operations".

With the Internet of all things, cyber-defense and security as a strategy become necessary and absolutely important as a legal framework, political framework, and economic framework of burden sharing at NATO.

At the same time, it will simply "market" NATO in the "smartest and easiest way" at a time of financially and socially emerging markets, where nonmember states require individual or tailored cooperation with NATO. It will facilitate NATO's expeditionary role for force projector, trainer, and crisis management operator, as an ". . .active leader in peace and security (NATO 2016)."

Cyber-Security Liability and NATO

NATO's role is expeditionary. We could state what NATO's role is as a force projector, force planner, force multiplier, force initiator, and force applicator. It does apply these "rules" for the benefit of a safe and secure environment when risk is constantly assessed (Efthymiopoulos 2008b).

Between the years 2001 and 2016, among others, the Alliance has responded through actions such as the following:

1. Invoking Article 5 (NATO 1949), as a consequence of the terror attacks in the USA, on September 11, 2001, claiming its right to defense against external aggression.

2. Allied states agreed on an everlasting transformation: political, military, operational, and strategic, as was approved during the Prague Summit of 2002 (NATO 2002),
3. Agreed to be involved in outer areas of traditional operations in Kosovo (NATO 1999), Afghanistan, in 2001 (Brookings Institution 2009) onward via operation in the International Security Assistance Force (NATO 2001).
4. NATOs Chicago Summit in 2012 and later on the Wales Summit of 2014 confirmed on a Smart Defence initiative, which is of qualitative and quantitate value, for, among others, agreed into joint interoperability efforts, including efforts to establish a concrete strategy and policy Cyber-Defence (Ibid 4).

In an emerging globalized world, where complexity may become the key characteristic in strategy and security, resilience will become an integrated part of NATO's policy orientation and application. New vulnerabilities and threats continue to emerge. Political pressure will require NATO leaders to take decisions about the organization's future. Yet all agree that NATO is a necessity. As such NATO should become more open, more adaptable, and more flexible. With more burden sharing, better smart budgeting, long-term planning and operational application, and continued success, NATO should continue be re-branded as an adaptive security organization, which does more to offer security and strategic alignment to truly current but also future challenges and threats that we may not yet anticipate or think of.

In the not so distant past, similar actions were reaffirmed in commitment to establish a policy and methodology, by the Heads of States and Governments, included, among others, the Treaty of London in the 1990 Summit, to the 1994 Summit in Brussels, and in 1999 over its fiftieth-year anniversary Summit in Washington, to the immediate decisions taken in 2001 after the terrorist acts in the USA (NATO 2001) to its sixtieth anniversary, which was held in Strasbourg and Kiehl accordingly in April 2009 to the Chicago Summit of 2012 and the Wales Summit of 2014, which added value to the Alliance and Allies reaffirming NATOs long-term necessity but now also strategic resilience to multidimensional challenges and threats.

Vulnerabilities and threats considering multidimensional challenges require NATO to be truly, strategically, and operationally agile. It requires NATO to be adaptable to conditions unforeseen.

Considering technological advancements, we are yet to acquaint ourselves, our institutions, our governments, and our international organizations with true phenomena of a new, yet networked, global society. In this borderless society, where electric grids, information, or installations failures may have in the past solely affect a country, they now affect a region and possibly a larger area. It may also affect global financial systems and social structures. Current financial situations in regions and areas, such as in the south of Europe, like Greece, Italy, and Portugal, among others, affect the larger European Union as a community of union states.

The refugee issue and the fear of mass illegal migration, deriving from current wars in Syria, Iraq, and other areas such as Afghanistan, affect countries, giving rise to suspicion on cooperative effectiveness and participation in defense against threats

and challenges. Even more so, when a global society is e-wired, in which education, training, health, but also security are part of this "grid," the threats and challenges are greater.

In this new virtual world of things, where the Internet has managed to eliminate distances and borders but also time, NATO should be set to comply with the new "global rules." It should create agile and limitless policies, security, and basic and specialized military and civilian installation if NATO is to continue to be a crisis management institution.

NATOs Resilience in Crisis Management and Communication

Societal security, an emerging phenomenon in the field of strategy and security, requires good crisis management skills but also communication effectiveness in both the real and virtual worlds. Business continuity at NATO requires, as foresaid the Alliance, to be resilient, and, surely for the purposes of this research paper, for the Alliance and allies to be cyber-resilient.

By methodological approach, societal vulnerability continues and will always continue to exist, so far and as long as threats are there. Considering the current civil need to be always preparing for a new "cold era," among others, considering the annexation by Russia of Crimea in 2014 (BBC 2014) and following the disintegrating relations of NATO due to the unlawful act of Russia to Ukraine, the establishment of the USA and then taken over by NATO, of the Missile installation in Romania (Reuters 2016) and the immediate reaction and accusation of Russia in regard to these developments (New York Times, "Russia calls new US Missile Defense system a direct threat", http://www.nytimes.com/2016/05/13/world/europe/russia-nato-us-romania-missile-defense.html, [seen May 5th 2016]), the refugee challenges as an outcome on the constant fight against ISIS (US Homeland Security Committee 2015), but also the phenomenal changes in the financial world (i.e., The Panama Papers (The International Consortium of Investigative Journalists (ICJ), https://panamapapers.icij.org/ [seen May 12 2016])), NATO is required to become truly resilient NATO, as should also nations and leaders.

All aforementioned elements are crisis management factors. NATO provides the tools and methodologies, in which Alliance members jointly agree to face strategic and operational challenges; to mitigate plans for crisis situations; to establish risk methods in a pre-crisis, during-crisis, and after-crisis situations; allies are to reach out for interoperable operational capacity building; logistics of deployment and information gathering; while jointly training for purposes, among others of a joined defense or attack under the rules of engagement and under article 5 of the NATO treaty.

In such similar cases, the legal and political perspectives also on cyber operations should be clear. The success of an operation lays to effective logistical and operational support. Therefore the legal aspects that come with sharing of information, on how to deploy forces and identify key threats and elements in cyberspace, are important. The Internet has no borders. And threats can be easily infiltrate the

national e-space and boundaries. Leaders are welcomed upon to take strong strategic-led decisions.

NATO is to ensure protection of all infrastructures. The Allies should be able to anticipate, identify, mitigate, and recover from "hybrid attacks (NATO Review, Hybrid War, Does it Even Exists? http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm [seen May 2 2016])" – the dimension(s) of simultaneous attacks – while reducing the threat of destabilization and or spreading fear.

In a civic society, it is our responsibility to ensure adequate awareness on cyber-defense and security. To learn about the necessity to protect all infrastructures, NATO's collective defense should be characterized by burden sharing, openness, flexibility, and transparency in cooperation and information flow among member states. Through preparedness and strategic and operational awareness, strategic resilience can be achieved. Response time and framework will then allow NATO to counter threats as they emerge.

Tendencies in the Cyber World

The twenty-first century is characterized by the use of advanced technology. By 2016, technology is merely a tool, interconnected with services provided through the Internet. Our wired society includes online services such as banking, communications, security services, shopping, and media services, to name a few, which now take place in cyberspace. These services are by now vulnerable to cyber-attacks. As countries steadily move forward in becoming dependent on technology and wider networks, the security stakes also increase.

Current security risk assessments consider that there is constant development of cyber-organized crimes that need to be countered. "Cyber-crimes" are executed by organized groups. Hackers are considered illegal users that know how to get access to personal, classified, or other unauthorized information by informal and unaccepted means at all levels and in all places. The use of personal, unauthorized, or private information to get access to other resources, such as funds or weapons, is a crime, as is the use of the web to terrorize citizens, states, institutions, or organizations.

In terms of applying these issues in military policy, through national or NATO command on cyber-defense policies, NATO or national armies use the Internet and technology to protect, defend, and secure governments, infrastructures, and people. Therefore, the creation of a cyber-defense policy was in fact a necessity and, more importantly, was seen as a necessity that we clearly pointed out following the first truly organized cyber-attacks in Estonia in 2007 (Cyber-Policy in Estonia: http://www.nato.int/cps/en/natolive/75747.htm).

> "...NATO has now moved on to help Allies improve their cyber-resilience by introducing capability targets into the NATO defense planning process and devising a new memorandum of understanding between NATO and individual Allies to establish secure connectivity and arrangements for information-sharing and crisis management... (Ibid 3)."

As pointed out by NATO Review, cyber-resilience is a tendency for building capabilities. Fields include but are not limited to network protection infrastructure, awareness and training and education, systems configuration, and infrastructure protection, among others (Ibid 3).

NATO's (CCDCOE) Cooperative Cyber Defence Centre of Excellence in Estonia, is the result of a full-scale cyber-attack, which occurred in 2007 (NATO Cooperative Cyber Defense Centre of Excellence, https://ccdcoe.org/ [1 May 2016]). Today, the CCDCOE is a center for excellence, that is supportive to NATO's operational and capacity building operations as well as legal operations reflecting cyber-space. It seeks security and defense resilience policies and capacity-building processes. Through its exercises and conferences, CCDCOE raises awareness on cyber-defense and cyber-security. An example is an important contribution to the national framework on Cyber-Security (National Cyber-Security Framework 2012), but also legal elements (CCDCOE 2016a) reflecting the framework for cyber-security and cyber-defense. The CCDCOE, seeks to establish standardization processes that were discussed in the Warsaw Summit in July 2016 and expected to be discussed in the July NATO Summit meeting of Heads of State and Governments. To allow for resilience in skill building of and about cyber-operators and the wider strategy on cyber-resilience. Once outcomes and results are accepted, they may expand to the appropriate NATO agency on standardization process, which is the NCIA agency "NATO Communications and Information Agency (NATO Communication and Information Agency (NCIA), https://www.ncia.nato.int/Pages/homepage.aspx [seen 2 May 2016])." The NATO Agency has as a core policy to adapt and standardize procedures. It follows the agreement at the NATO Warsaw Summit of Heads of State and Governments and allows for better coordination and collaboration with the market stakeholders.

NATO's Concept of Cyber-Defense

It was NATO's Military Committee decision to adopt a "Cyber-Defence Concept" (Ibid, 4). The Committee's aim was and still is to deliver business continuity and military resilience. As NATO is a provider of collective defense and as a collective organization in a globalized and currently unsafe e-world, it needs to be agile. In a global environment of insecurity, NATO Alliance delivers security methods. It takes into perspective new forms of asymmetrical threats, such as cyber-attacks.

Historically, the 2002 Prague Summit first marked NATO's tasking authority committee with regard to all activities that should be held in relation to cyber-defense. As technical achievements were delivered so policy-makers delivered policy results on cyber-defense. That is why Allied leaders during the Riga Summit of 2006 acknowledged the need to include these as is stated on its decisions at the Press Communiqué (1) to protect NATO's operational information systems and (2) to protect its allied countries from any e- or in other words cyber-attacks by new forms and means developed by NATO's Allied Command Transformation (ACT) In Norfolk, Virginia.

The output of the informal Meeting of the Ministers of Defence in October 2007 of NATO (NATO Defence Ministers Meeting 2007) gave way to the inauguration of NATO's Centre for Excellence (COE), which at a later stage got accredited to have become the Allied Command Transformation on Cyber Defence, named as Cooperative Cyber Defence Centre of Excellence, CCDCOE (NATO 2008b). It was based, on the concept and early understanding of cyber-resilience for NATO's future policies in countering challenges and threats, as was agreed by NATO's Military Committee.

The central and final decision-making role over the policy of cyber-defense, however, is done by the North Atlantic Council (NAC), which accordingly is led by heads of state and governments. This is the highest deciding political authority which decides, creates, and overviews policy. It also evaluates, considers, and adopts NATO's policies and activities with regard to political and military affairs or standing issues on challenges and threats, among others. Below the NAC is NATO's Consultation Control and Command Agency (NC3A) (NATO NC3A 2002) now transformed to the NCIA agency (Ibid, 44) and the NATO Military Authorities (NMA). The latter authority has implementation as its major task (NATO's Cyber-Defence policy 2008).

The implementation of NATO's cyber-defense policy is considered as the second most important decision by now, once the decisions are taken by the NAC. The "Concept of Cyber-Defence" "adds practical action programmes, to fit within the overarching policy" (NATO 2009). The "Cyber-Defence Management Authority" that is tasked upon its policy concept "brings together the key actors in NATO's Cyber-Defence activities." Its aim is to manage and support all NATO communication and information networked systems and individually allies upon request (NATO 2008c).

NATO's policy creation and activity are "encouraged" by Allies. The objective is to adapt the Alliance to new strategic and security environment challenges, that are "hybrid," to engage as many as possible governments, industry-related market companies, and individuals. In accordance to its best practice policy, NATO considers that its "operational forum" can and should be considered as the best joint operational cooperation between states and market, as to also avoid duplication of efforts and use the necessary global knowledge to achieve interoperability of force action and command also in cyberspace.

Practically, in military policy, implementation, or operational areas, NATO has adopted "three phases of practical activity and cooperation": the initial phase includes a NATO Computer Incident Response Capability (NCIRC). It was established as "interim operating capability" for NATO to build up on both security risk and manage the element of cyber-threats. Its second phase involved an ever more realistic and pragmatic perspective that required the coordination of all initial "offering" states to the attempt to establish a cyber-center (under the NATO agreement between states of a voluntary national contribution –VNC) in bringing the NCIRC to a full operational capability (Ibid).

From that point on, it became an administrative decision of the Allies that once the aforementioned stages would be put into effect, then a third phase would come into existence: needless to say, this third phase was a complete implementation and

rule-based operational procedure that would soon enough bring about into existence NATO's request for technological agility and resilience, which are also yet to be finalized at the Warsaw Summit of July 2016. "It consists of incorporating – lessons learned – from the prior two phases as using new and latest Cyber-Defence measures (use of new technology and getting more knowledge on the security environment), in order to enhance Cyber-Defence posture. Once the third phase was evaluated, the Allied Command Transformation (ACT) decided, to accredit the operational center – in this case the Cooperative Cyber Defence (CCD) COE (Estonia), what is called as a 'Centre of Excellence'-. In turn, this resulted to the inauguration of the CCDCOE by May 2008."

Cyber-Defense Put to the Test: The Estonian Case of 2007

The Centre of Excellence in Tallinn was primarily supported for two reasons: (1) it was already scheduled by the time of its inauguration as an idea. Estonia would have been the host country for such an operational center. Today the Centre of Excellence is yet to welcome more members, the latest ones to join being Greece, Turkey, and Finland (CCDCOE 2016b). (2) Estonia had already been a witness of modern asymmetrical hybrid warfare attacks by 2007. It is estimated that what triggered an attack from inside and outside the country's infrastructure was the action of Estonians removing the bronze statue of a Red Army soldier, during the Soviet times, from the center of Tallinn. It was an honorary statue, honoring the dead of the Second World War. This matter sparked social outrage between Russian-speaking populations (News Scientist, 2007). It resulted to continuous cyber-attacks on Estonia's e-infrastructure, public and private and military and civilian.

By 2008, seven Alliance countries according to the Memorandum of Understanding on the cyber-defense center supported Estonia to get full operational capability (Germany Italy, Latvia, Lithuania, Slovakia, and Spain), which lead to an evolution period. By 2016, NATO Allies are expected to discuss further and finalize the framework, logistics and operations, elements of cyber-resilience, and procedures on the policies, when considering threats and challenges in a changing environment. NATO is yet to decide on the resilience policy, as hybrid warfare is developing, at a time when Smart Defense of NATO nations is expected to achieve the goals and aims which are to be seen by the year 2020.

The cyber-attacks in Estonia of 2007 are still today the biggest and most organized electronic attack, with a duration period of several weeks, which provided NATO with a motive and multipurpose task for years to come. NATO's leadership was in fact correct in its judgment that (1) such an operational center and policy was needed and (2) its operational center would constantly be evaluating and evaluated. Research would enable progressive evolution in cyber-defense and security, while provide technological advancement and agility in malware, and cyber-security law, among others.

The inauguration of its Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, in May 2008, led to a mission, which holds a clear

vision and statement. It is yet to be "politically ratified" and adopted as a key core policy by Allies. Its raison d'être as stated is "to enhance the co-operative Cyber-Defence capability of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative Cyber-Defence," therefore reflecting on the key core elements to counter-hybrid threats and being constantly resilient to strategic requests and needs. The vision is for the CCDCOE to become "a specialized and expertise center for NATO in cooperative cyber-defense (CCDCOE, Training Catalogue, https://ccdcoe.org/sites/default/files/documents/Training_Catalogue_2016.pdf)."

The domain of the cooperative cyber defense center in the framework of cooperative security within NATO focusses in the fields of research which include:

- Legal and Policy elements
- Concepts and Strategy
- Tactical Environment
- Critical Information Infrastructure Protection (Ibid, 41)

The Centre's core policy created an outcome of research and policy orientation, as already analyzed. It was presented primarily as a first outcome then accepted by the Supreme Allied Commander Transformation (SACT), deriving from a request of NATO HQ (headquarters) and by the North Atlantic Council (NAC) level. This included a strategic doctrine and concept development, awareness and training, research and development analysis and lessons learned, and finally consultation. Now we are at the stage of heads of state agreement as policy and action reflecting the key core policy of NATO resilience to counter emerging challenges, a procedure that will be discussed, negotiated, and agreed upon by consensus by the Allies in Warsaw.

NATO Approaches Issues Relevant to Cyber-Security

For the concept of cyber-defense, the Centre for Excellence in Tallinn continues to portray and project NATOs need for a methodological cyber-resilience policy. If agreed, at the upcoming NATO Warsaw Summit, cyber-security will become NATOs core policy. It will be an integral part of Smart Defence in the hope to enhance the cooperative defense system.

The ideology and methodology behind the policy recommendations are not a new one. As an example by February 6 and 7, 2009, NATO's Science for Peace and Security (SPS) sponsored a workshop. It foresighted a similar argument which we also recommend in our paper that cyber-security approach and cyber-defense are and should become a core policy of resilience at NATO.

The workshop titled "Operational Network Intelligence: Today and Tomorrow" aimed at adaptation knowledge procedures considering the evolving and fast-growing technology. Its overall purpose was "to rethink present strategies and identify urgent measures to be taken in order to minimize the strategic and economic

impacts of cyber-attacks" (NATO 2009). This was the level of anticipation at the time, considering future correlation of Smart-Defence with the policy of cyber-defense at its core.

Considering risk processes and assessments on hybrid threats and challenges (Davis 2015) but also the need for better civil awareness and readiness, at a time of much needed cooperative defense, Allies have to decide for a robust long-term planning strategy and operations of NATO, keeping in mind the need for strong success in field operations, including success in and at a multidimensional level of operations against all threats.

NATO increasingly recognizes that organized cyber-attacks seek to take advantage of "gaps" in the "system social and market matrix." Therefore it should be a request from member states to examine the increasing need for coordination of human factors related to the issues of electronic warfare, operational network, intelligence, and Cyber-Defence, whether for training, scientific exchange, and or operations.

NATO is currently using people involved in e-systems, security, IT engineers, researches, officers dealing with network operations, and operational centers as well as professional and academics. Specialists in the field on both a strategic and tactical level should be systematically involved at organized levels of research, sharing, discussion, and exhibition of outcomes, which will in turn enrich the abilities, capabilities, and capacities of rendering current smart-defense and cyber-defense as a key and successful resilient and collaborative defense policy to NATO.

Proposals

NATO's level of ambition considering a much needed resilient policy in cyber-defense should be decided upon the Warsaw Summit of 2016. Specialized policy against hybrid threats should be adopted. A specialized commitment of Allies to share information and simplify procedures for cooperation with cyber-companies in electronic warfare should increase.

NATO should and could do more, on a strategic level, by:

1. Sharing concrete information on security led affairs of cyber-defense within and among member states but also with non-NATO members.
2. NATO should enhance global cooperation with nonmember states in the field of electronic security and safety, as there is an increase of cooperation level, such as the UAE (NATO and the UAE determined to enhance cooperation, (March 2016), http://www.nato.int/cps/en/natohq/news_128753.htm, [seen May 10th 2016]).
3. Allies at the upcoming Warsaw Summit meeting in July 2016 should jointly agree on a robust and resilient cyber-defense policy, in which CCDCOE should stand out as a tool for NCIA cooperation methodology for smart defense achievement.

4. NATO should hold a clear budget on smart defense, based on the technological necessities that allow lower but shared budgets for the long-term and a policy of cyber-defense that look operationally viable and globally market-oriented.
5. NATO should reach out for interoperability levels for NATO forces 2020 Smart Defence standards as well for cyber-defense.
6. Through joined cooperation at the level of electronic warfare prevention, detection, and reaction to attacks toward member allied states, the duplication of efforts by nations can be avoided.
7. Legally, cyber-resilience can be achieved through clarification of what constitutes an e-crime or e-terrorist attack. It should be clarified if not yet done so and adopted not only by Allies but proposed at the level of the United Nations for universal adaptation.
8. The capability and/or capacity for NATO to operate under rules and regulations of traditional rules of engagement in an e-world should be clarified; It is also necessary to clarify the tools and infrastructures that are or will be used for such operations conforming with a universal law on cyber-defense and cyber-security methods and actions that is yet to be defined from the United Nations and sub-expert committees.

It is crucial for NATO to achieve interoperability of force command and structures through a methodological application.

Tactically, NATO needs to do the following:

1. Adopt an operational policy procedure reflecting hybrid threats in a cyber-environment.
2. Tactically align new policies with regulatory agreements based on NATO's regulatory and strategic rules, relating to defense clauses and rules of engagement.
3. An assessment on future warfare should be considered and agreed upon.
4. A foresight agency which provides prime information on constantly evolving technology, robotics, and smart attackers should be created.
5. As NATO holds a joined center for warfare, so should NATO be proposed to have a cyber-resilient military operational command and control center on electronic warfare; it will apply current rules and regulations, consult the CCDCOE, and provide a time action plan for a hybrid threat assessment accreditation on cyber-NATO standards.
6. NATO should allow for alliance progress through resilience on all operational levels which involve the creation of interoperable cybernetic command structure and technologically agile forces for all levels of "analogical and digital" engagement of forces in electronic warfare.
7. NATO should enhance its national protection plan of major infrastructure through a complete and jointly by consensus agreed cooperation of national states.
8. NATO base infrastructures should be resilient and be constantly ready-protected from possible fraudulent attacks.

Conclusion

In conclusion, the main aim was to project the importance of cyber-resilience at a time of NATO's strategic evaluation. The aim was to methodologically approach how to integrate NATO's collective defense, through cyber-defense policy, to the twenty-first challenges and threats.

In anticipating the outcomes of the upcoming Warsaw Summit meeting in July 2016, NATO's resilience policy, if adopted to become an integral part in cyber-defense as well, will constitute a methodological and strategic change for NATO. NATO's smart defense and collective defense overall will have to be reexamined to meet the high expected standards of security. It will create a new standardized form of procedures, adaptable to the reality of risk hybrid assessments and threats as analyzed in the paper. NATO will be able to afford flexible strategic and operational forces agile and technologically advanced.

The creation of a concept and later policy of cyber-defense and the inauguration of the Centre of Excellence for Cyber Defence in Tallinn Estonia in 2007 provided an early impetus for future operations but also administrative and operational upgrading in the field of today's smart defense policy a result of the renewed strategic concept.

Cyber-defense is a policy within the framework of NATO. Yet it is not a key core policy just yet until the final results of the Warsaw Summit meeting.

This article aimed to show why cyber-defense should become a core policy for resilience at NATO. The article conceptualized from a strategic and policy concentration. It analyzed the policy of smart-defense, cooperative defense, cyber-security, hybrid threats and crisis management, and communication, among others. It examined strategically overviewing current, past, and future events to come. It assessed and concluded that there is a growing necessity for constant protection against current of future challenges and threats which are now multidimensional, and as such NATO should be adaptable at all times.

The policy of cyber-defense through the prism of Smart Defence allows for a truly and united allied effective engagement, an engagement that should be operationally resilient in military operating environments at all levels. On the way to adapt to the cyber-realities of the Internet of all things, NATO should adopt a legal and political framework and a tactical and operational framework in a methodological easily adaptable way that compete the current and future as we referred to hybrid challenges and threats. Any decision made at the level of heads of state and government should include the legal element of operation. As cyber-threats are borderless, so should NATO work as an operational and capacity-building organization that does more to provide effective crisis management solutions through a wide range of nations cooperations, which are NATO and non-NATO members, when national and supranational security of allies is or may be compromised.

The outcomes of this chapter, provided the reader with an updated information on cyber-security and cyber-defense issues, within 2018; We reflected on Smart Defense and more so, examined the case of NATO as an international organization

at the level of resilience, strategy, and tactics. We recommended proposals for strategic and tactical consideration, reflecting current and future situations namely in the capacity management building, administrative decision training, and making on Cyber-Security; limiting fiscal costs, and leveling operational methods in cyber-defense in current or future networked operations, elements that will be evidently shown in the July 2018 NATO Heads of State and Government Summit meeting.

References

BBC. (2014). Crimea profile. http://www.bbc.com/news/world-europe-18287223. Seen 10 May 2016.

Brookings Institution. (2009). Afghanistan: The Taliban Resurgent and NATO, Published by Brookings Institution, March 31 2009. http://www.brookings.edu/opinions/2006/1128globalgovernance_riedel.aspx

CCDCOE. (2016a). International norms of cyber-security. https://ccdcoe.org/international-cyber-norms-analysed-new-book.html. Seen 12 May 2016.

CCDCOE. (2016b). Greece, Turkey and Finland to join the CCDCOE. https://ccdcoe.org/greece-turkey-and-finland-join-nato-cooperative-cyber-defence-centre-excellence.html

Chicago Council on Global Affairs. (2012). Conference: *Smart defence and the future of NATO, can the alliance meet the challenges of the 21st century*, March 28–30, 2012, Chicago.

Davis, J. R. Jr., Major. (2015). Joined warfare center, "continued evolution of hybrid threats". *Three Sword Magazine*, 28 2015. http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf. Seen 12 May 2016.

Efthymiopoulos, M. P. (2008a). JIW Vol. 8, Issue 3, (Journal of Information Warfare), *NATO's security operations in electronic warfare: The policy of cyber-defense and the alliance new strategic concept*. Australia, http://www.jinfowar.com/

Efthymiopoulos, M. P. (2008b). *NATO in the 21st century: The need for a renewed Strategic Concept and the ever Lasting NATO-Russia relations*, Athens, Thessaloniki, Published by Sakkoulas A.E. (in Greek).

Efthymiopoulos, M. P. (2013). Chapter in cyber-development, cyber-democracy and cyber-defense. In E. G. Carayannis et al. (Eds.), *NATO's cyber-security policy.* London: Springer.

Hughes, R. B. (2009). Atlantisch perspectief, Ap:2009 Nr. 1/4, *NATO and cyber-defense: Mission accomplished, Netherlands, Netherlands Atlantic Committee.*

Kramer, F. D., Binnendijk, H., & Hamilton, D. S. (2016). *NATO's new strategy: Stability generation*. Washington, DC: Atlantic Council of the USA, Brent Scrowcroft Center on International Security.

National Cyber-Security Framework. (2012). NATO Science for Peace Program. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. Seen 14 May 2016.

NATO. (1949). *NATO treaty: Basic document of the treaty.* http://www.nato.int/docu/basictxt/treaty.htm#Art05

NATO. (1999). *Operation allied force on Kosovo*. http://www.nato.int/issues/kosovo_air/index.html

NATO. (2001a). *International security assistance force (ISAF)*. http://www.nato.int/isaf/index.html

NATO. (2001b). *Information on immediate NATO reaction*. http://www.nato.int/docu/update/2001/0910/index-e.htm

NATO. (2002). Prague summit. http://www.nato.int/docu/comm/2002/0211-prague/. Assessed 4 May 2016.

NATO. (2008a). *Briefing on transforming allied forces for current and future operations*. Brussels: NATO Public Diplomacy Division.

NATO. (2008b). *CCDCOE*. From http://www.ccdcoe.org/11.html

NATO. (2008c). *NATO defence against cyber attacks*. http://www.nato.int/issues/cyber_defence/practice.html
NATO. (2009a). *A road map to the strategic concept of NATO*. http://www.nato.int/strategic-concept/index.html
NATO. (2009b). *SPS workshop rethinks approaches to cyber security*. http://www.nato.int/docu/update/2009/02-february/e0206a.html
NATO. (2016). *Operations and missions: Past and present*. http://www.nato.int/cps/en/natohq/topics_52060.htm. Seen 4 May 2016.
NATO Defence Ministers Meeting. (2007). *Informal meeting of NATO defence ministers*. http://www.nato.int/docu/comm/2007/0710-noordwijk/0710-mod.htm
NATO NC3A. (2002). *NC3A agency*. http://www.nc3a.nato.int/Pages/Home.aspx
NATO Review. NATO defense and cyber-resilience. http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/. Assessed 23 Apr 2016.
NATO Warsaw Summit. http://www.msz.gov.pl/en/foreign_policy/nato_2016/. Seen on 22 Apr 2016.
NATO's Cyber-Defence policy. (2008). *Defending against cyber-attacks*, focus areas. http://www.ccdcoe.org/37.html
NATO's Cyber-Defense Policy. (2011). http://www.nato.int/cps/en/natolive/topics_78170.htm
NATO's Smart Defense policy: Smart Defence is a cooperative way of thinking about generating the modern defence capabilities that the Alliance needs for the future. http://www.nato.int/cps/en/natohq/topics_84268.htm. Seen on 26 Apr 2016.
Rehman, S. (2013, January). Estonia's lessons in cyber warfare. *US News*. http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare
Reuters. (2016). US activates Romanian Missile Defense. http://www.reuters.com/article/us-nato-shield-idUSKCN0Y30JX. Seen 12 May 2016.
Sendmeyer, S. A. (Maj). (2010, August). *NATO strategy & out-of-area operations*. School of Advanced Military Studies, US Army Command & General Staff College. http://www.hsdl.org/?view&did=713508
US Homeland Security Committee. (2015). *Syrian Refugee flows, security risks and counter-terrorism challenges*. https://homeland.house.gov/wpcontent/uploads/2015/11/HomelandSecurityCommittee_Syrian_Refugee_Report.pdf. Seen 5 May 2016.

Focusing on Mission and Business Objectives Through a Different Lens: The New Cyber Offensive

45

John S. Hurley

Contents

Abstract

The blueprint for engaging in cyberspace has largely been designed and implemented by the military due to the nature of its roles and responsibilities. On the global stage, safety, security, prevention, and resolution of conflicts generally fall squarely within the purview of the military. Conflicts and challenges in the traditional domains of engagement (air, space, land, and maritime) can usually be viewed in and approached from an apples-to-apples context by the military. However, the cyberspace domain because of its inherent asymmetry and low requirements for entry requires that the public and private sectors be viewed as viable participants and combatants. In addition, unfortunately, these two sectors also provide an incredibly rich target space. The military culture has viewed cyberspace primarily from a defensive and reactive posture. However,

J. S. Hurley (✉)
College of Information and Cyberspace, National Defense University, Washington, DC, USA
e-mail: john.hurley@ndu.edu

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_46

cyberspace dictates that a much broader position is taken because the public and private sectors require and provide different context and scales that fall outside of the military's normal scope and obligations. Offensive cyber operations are spoken of only in very select circles and most likely in retaliation and secondary to mission and business priorities and objectives. In this effort, I will provide a "new" perspective on cyber offensive operations and how they can be used to better address mission and business priorities. The case studies utilized in this effort show that mission and business priorities can not only be addressed proactively but also yield significant benefits to organizations, agencies, and communities if offense is viewed through a different "lens."

Keywords
Conventional · Critical infrastructure · Cyberpower · Cyberspace · Data · Data-driven · Information · Information society · Mission · Objectives · Offense · Operations · Power · Weapons

Introduction

Cyberspace, first coined by William Gibson in his novel Neuromancer, describes an advanced virtual reality (VR) network in which data are abstracted from the banks of every computer in the human system (Gibson 1984). Gibson considered this domain to be unbounded by distance or any other physical limitations, i.e., a "nonspace" that lacks the physicality conventionally implied by "space." Gibson suggested that cyberspace was a place shared by multiple disembodied minds – a collective hallucination. To be clear, this view represented a revolutionary wave of thought in which there was a complete disassociation between the real physical world as we know it and the digital world. In this context, cyberspace is viewed as a commons in which information could be shared by anyone, any place, and at any time. Gibson's, at the time, outlandish premonition has now evolved into our contemporary culture in a way that very few could have predicted. This notion paralleled the thinking of a number of the brilliant minds in academia and industry. In particular, the contributors responsible for the development and deployment of the Internet and the world wide web (www) (Leiner et al. 2017; Berners-Lee 2017) were key in achieving the realization of Gibson's cyberspace concept in our time. It is important to note that the academic and private sector communities were not the only major players involved in this endeavor. The role of the Department of Defense in this undertaking cannot be understated.

As history reminds us, the Department of Defense (DoD) was a major stakeholder in the information technology (IT) revolution and many other relevant developments through its provision of many of the resources and facilities that enabled much of the research and development to eventually translate into the environment that Gibson predicted. As a major investor and contributor, DoD (the military, in particular) recognized the potential for this information environment to be a warfighting domain in which long time enablers (e.g., networks, computer systems, radios) could also

serve as weapons platforms from which attacks could be launched and information advantages be achieved. In terms of cyberspace operations, the joint staff views cyberspace as "a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Cyberspace Operations 2013). The challenge, however, is that these weapons platforms are capable of being used by any and all with the capability and intent, including friend and foe alike (Quick 2014). As a result, cyberspace has been the subject of much discussion by senior leaders in strategy sessions within the defense and intelligence communities for several decades. As might be expected, perspectives on cyberspace differ from community-to-community due to a number of different factors.

Cyberspace has been framed through different lens by each of the three communities that often highlight their disparate values, roles, responsibilities, duties, and priorities. Historically, the differences have resulted in a schism between the federal government (in particular, DoD) and the public and private sectors. The different views, policies, and resulting approaches by the federal government have contributed to irrefutable levels of mistrust between the three sectors, in which the federal government's motives and agenda have been constantly questioned by the public and private sectors. It has primarily boiled down to issues of control, accountability, and responsibility. For example, when the subject of cybersecurity arises, there is a general agreement between each of the communities of the need to improve upon existing conditions. However, solutions and approaches to achieve success are major issues of continuing debate between the sectors. The World Summit of the Information Society (WSIS) in 2003 and 2005 in Geneva and Tunisia, respectively, identified a number of major pillars that were agreed between the members from various sectors in attendance. From December 10 to 12, 2003, in Geneva nearly 50 heads of state/government and Vice Presidents, 82 Ministers, 26 Vice Ministers from 175 countries, as well as high level representatives from international organizations, private sector, and civil society attended the WSIS Geneva phase. From November 16 to 18, 2005 nearly 50 heads of state/government and Vice Presidents and 197 Ministers and Deputy Ministers from 174 countries as well as high level representatives from international organizations, private sector, and civil society attended the WSIS Tunisia phase (WSIS+10: WSIS Review Process 2005). WSIS represents a bold attempt to present the issues raised by information and communications technologies (ICTs) through a structured inclusive method (WSIS+10: WSIS Review Process 2005). In these two historic meetings, a number of the pillars of society, as a whole, were identified and agreed upon by the three sectors that could yield a unifying consensus. Security and confidence were identified as main pillars of an Information Society, speaking to the unanimous position that society, as a whole, wants to be secure and safe. In addition, confidence reflected the view that there should be an ability to achieve and improve upon the quality of life.

The explosion of data predicated by the development of new technologies has created a need for the communities to use and incorporate data to meet many of the demands and opportunities created by the massive volumes of data generated.

Though priorities, culture, and mission highlight many of the stark differences that separate the three segments of society, a shared and common need, as suggested through the WSIS summits, can provide promise for consensus and cooperation to overcome many of the differences between them. In this effort, such a common and shared thread is proposed that translates through culture, tradition, and mission that can enable synergy to be achieved. The effort starts off with the discussion of power and how though it can have a similar meaning, can be used and interpreted quite differently across the communities. Next the focus is on cultures and how their roles and responsibilities can disconnect them. In particular, offense (specifically offensive operations) means something totally different to each of the communities and serves as the focus of this effort, i.e., seeking a new cyber offensive that permeates across the sectors. Cyberspace and how it has leveled the playing field in terms of how power is wielded is next. The data explosion and its impact on society are then considered, and it is then followed by the proposed common thread. In the conclusion some new ways are proposed to address and meet the consensus required to move our society into a more productive era.

Power

Power can be defined in a number of different ways, including (1) the ability to do or act, capability of doing or accomplishing something; (2) political or national strength; (3) the possession of control or command over others; (4) authority; (5) ascendancy; etc. (Power 2017). Of particular interest are (2) and (3) because regardless of the segment of society involved, strength, authority, and control have been constants in discussions of power. However, though there are some important undeniable common views on power shared by the different segments of our society, it is vital that the concept of power be considered in the appropriate context. This point is crucial because the three segments of our society can at any time have totally different priorities based on their desired outcomes and the relevant situations. For certain, in the USA, the federal government, private sector, and the public domain have shown very different ways in which they see power and how it is applied largely due to their different priorities and expectations. Power is often linked to results or to the means for achieving the results. Again, context is extremely important because for the military, power and authority are often discussed in the context of "war" – a domain less familiar to the public and private sectors.

When it comes to war, the military has generally been given "free" reign to make and execute decisions because of longstanding tradition and the exceptional job it has done, for the most part, over its history. The authority has been "shared" between the different branches of the federal government and the military. However, in reality, the authority seems to have rested primarily with the military for key decisions and courses of action. Some of this is largely due to "war" having been the principle responsibility of the military in the traditional four warfighting domains, i.e., air, land, maritime, and space. The other reason may be because war, at least in the conventional sense, has some very unsettling and uncomfortable

aspects that the rest of society would prefer not to see or be directly involved. The rules have changed dramatically as we consider now the fifth domain of opportunity and conflict, cyberspace. This domain presents a significant departure from previous battlefields in that the terrain or location of battle has expanded from conventional battlefields and targets where the rules are generally agreed and understood by combatants to a different environment altogether, mainstream society.

Instruments of National Power

National power, which stems from different elements or instruments or attributes, can be defined also in terms of all of the resources that a nation has at its disposal to pursue national objectives. These instruments fall basically into two groups as they relate to origin and applicability, i.e., "national" and "social." Social elements consist of areas such as: economic, political, military, psychological, and informational. National, on the other hand, consists of areas such as geography, population, and resources. Instruments of national power are used in the USA to achieve national strategic objectives and subsequently advance national interests (JP 1: Doctrine for the Armed Forces of the United States 2013). The instruments of national power that have been used most often are diplomatic (D), informational (I), military (M), and economic (E) or more commonly recognized by the acronym, DIME. The principal element of engaging with nations and foreign entities is through diplomacy, a primary means of advancing US interests, objectives, and values abroad and to solicit foreign assistance in US military operations. In addition, diplomacy is the primary way to organize coalitions and alliances while generating support among states and nonstates. The informational element used to be considered primarily in the context of traditional nation states. Non-nation state entities received much less attention. However, technology has not only significantly raised the profile of non-nation state actors but also blurred typical geographical boundaries that used to protect US interests. The informational component has become more important because of how it is interpreted both at home and abroad. The communication exchanged through various outlets, e.g., voice, social media, images, etc., can provide unintended consequences simply because it has been linked to the US government.

For the military, power is defined in terms of the resources that a nation state can mobilize against other nation states for the purposes of military deterrence, defense, and war. There is often a discussion of power in the military in terms of national power, which reinforces the ability of a nation to coerce other nations through the use of military means or to resist such coercion by other states. National power is then described in terms of two components, i.e., mobilized military capabilities ready for immediate operational commitment; additional power potential or the ability of a nation to produce further military capabilities. Fortunately, often military power does not have to be exerted to produce desired results. In some cases, the mere threat of military power has become a popular deterrent that has caused other nations and potential adversaries to reach "reasonable" conclusions that avoid conflicts instead of

promote them. It is important to note that following World War II, the concept of "war potential" started to gain traction and became more contextually "relevant" in discussions of national military power. This is significant in the current discussion because of how often power in the military is linked to war. World Wars I and II were won due to potential in manpower and economic resources (Military Power Potential 2017).

The military element of national power supports national security goals both at home and abroad. Fundamentally, the military instrument is coercive in nature and generates effects through the application or threat of force to compel an adversary toward a desired course of action or to prevent the U.S. and its interests from being compelled. This is important because the military instrument of power can reveal itself across a continuum of engagement that varies depending on whether the nation is at peace or war. The ways can present themselves in several forms including combat intensity, purpose, risk, and scale. Lastly, a strong national security and a strong economy are inherently related in ways that highlight the significance of the economic element of power. Historically, the major players in the world were those who had strong militaries and vast economic resources. During the cold war era, the major global powers or global titans in the world were the United States and the Soviet Union, nations that far exceeded most others around the world in terms of military might and economic resources (JFODS4: The Joint Forces Operations & Doctrine SMARTbook 2015). Discussions about power, as it relates to the military, will now be linked to conventional weapons and their use in war.

Conventional Weapons and War

DoD and the Intelligence Communities

Weapons have a unique history that began as far back as the thirteenth century. The Chinese are recognized as having invented the first weapon in thirteenth century A.D., a firearm that used the black powder invented by them in nineth century A.D. Conventional weapons, as we know them, have evolved significantly over time due to advancements in science and technology. In militaries around the world, especially in well developed countries, a diverse cache of weapons are on display, framed largely in the context of the services, e.g., Army, Navy, Air Force, Marines, Coast Guard, etc. (Weapons 2017). In addition, weapons are classified in accordance to specialization, including machine guns, cannons, rockets, mortars, grenades, and aerial weapons, etc. (Weapons 2017). DoD (and in particular, the military) and intelligence agencies recognized the value of information in the context of war. Two concepts that are worth discussing are information in warfare and information warfare (IW). Information in warfare embraces information in support of decision-making and combat operations. In IW, on the other hand, information is used as a weapon in and of itself in the context of warfare (Whitehead 1999).

Recently, adversaries have raised the profile of IW as a serious threat because of its potential use against US forces or the US homeland. Advancements in technology have created new resources and tools that have provided advantages for targets and

adversaries alike. Along with the vulnerabilities identified are opportunities that should also be realized with the advent of these tools and resources. There has been less discussion about the opportunities than the vulnerabilities largely due to two factors. Opportunities can be divided into two categories: (1) broad policies and strategic-implementation work and (2) highly technical feasibility studies. The feasibility studies are often classified and highly compartmentalized and the policies and strategies are often too general to be of any specific use to military planners (Nichiporuk 2002).

The issue of context has been a very important one that has been stressed throughout this work. Context has been used to explain a number of different topics including the rationale for some of the approaches used by the military in performing its duties. Part of the challenges that it faces is directly associated with its responsibilities and how it defines or seeks to define its roles with respect to the rest of society. Weapons are used primarily in the military for mission-related activities and except for a select segment of our society, such as law enforcement, hunters, and collectors, etc., there is little connection with the use of weapons. The military activities can be relevant to either offensive or defensive operations or some combination thereof depending on the requirements of the mission. There has been a longstanding disconnect between the military and the public and private sectors because industry and citizens do not, in general, talk in the context of weapons in the same way as the military except under very rare occasions. The differences are exacerbated even more when the discussions move away from safety or protection.

The military is focused on a narrow mission, i.e., protect and defend the interests of the United States and its allies. In addition, the military's views and beliefs have been shaped by generations of training, culture, intuition, and experience. The military's perspective places it at times in direct conflict with that of the public and the private sector who are not generally involved in conversations about actions driven by the need to use weapons or the goal of defeating or destroying an enemy. There is little question about the success and the results of the US military over time in its role of protecting the interests of the two communities that at times finds itself at odds. However, the military's approach and bottom line can for some of the reasons as those listed above be outside of the understanding of the other two segments of society. At times, the military and the other two segments seem to be talking past each other, with no necessary blame assigned to either party. It is just the reality of the times in which we live. As a result, it is important to take a closer look at society as a whole and how it has evolved to the present point.

Though the focus has been largely on the DoD community and the military, in particular, it is imperative to see how the intelligence communities have used information. The primary missions of the intelligence community (IC) are "to reduce uncertainty and provide warning about potential threats to the national security of the United States, the safety of its citizens, and its interests around the world." Decision makers – from the White House and Capitol Hill to battlefields and local jurisdictions around the globe – demand and depend on information and insights from IC analysts (Challenges for the Intelligence Community 2011). The military, with intelligence needs, for a wide variety of missions and officials, including the Office

of the Secretary of Defense, the Joint Chiefs of Staff, commanders of tactical operations, and designers of equipment and tactics, has been for obvious reasons the IC's most dominant customer. Although strategy and tactics are very important, it is also crucial to consider operations (defensive and offensive).

Defensive Operations

Defensive operations, though they normally cannot lead to a final decision, they can however buy time, economize forces, develop conditions favorable for offensive operations, and defeat an enemy attack. The purpose of defensive operations is to create conditions for counteroffensives that allow the initiative to be regained. Offensive support operations and stability are usually included in operational level defensive operations. Successful defenses use direct and indirect maneuvers in their aggressive approaches. Commanders use information operations, maximize protection, firepower, and those maneuvers that facilitate the successful defeat of the enemy. Mobile and static elements of operations, individually, enable commanders to resist and contain the enemy. Even more powerful when they are combined, these elements deprive the enemy of the initiative.

Technology advancements over past decades have significantly altered the way that commanders carry out defensive operations by enabling the forces to evolve, as well as, contribute to the way that commanders conduct defensive operations. Some of the benefits are the achievement of greater understanding of: intelligence, surveillance, and reconnaissance (ISR), combat service support (CSS) technologies, fusion of command and control (C2), and friendly and adversarial situations. However, the limitations of defensive operations provide an impetus for commanders at every available opportunity to seek to transition to offensive operations. Defensive operations, used by commanders either individually or collectively to improve situational awareness, can be placed into three different categories, i.e., area defense, mobile defense, and retrograde. Area defenses focus on sustaining position by drawing the enemy into a series of interlocking positions that makes the enemy vulnerable to attack. In mobile defenses, the enemy is lured into a position that exposes the enemy and makes it susceptible to being overtaken. Lastly, retrograde defenses enable friendly forces to be re-positioned in order to gain benefits of time, place the enemy in more vulnerable positions, preserve forces, and avoid combat when the conditions are unfavorable (Defensive Operations 2017). Next there is a focus on offensive operations, whose goal is to defeat or destroy the enemy.

Offensive Operations

Offensive operations are characterized by surprise, concentration, tempo, and audacity. By imposing will on the enemy and achieving decisive victory, offensive operations serve a very important purpose, i.e., achieve the decisive results in war. In defeating the enemy decisively, offensive operations seek to exploit, retain, and seize the initiative to defeat the enemy. Offensive operations should end when either force achieves the operation's purpose, approaches culmination, or reaches a limit of advance within the operational framework (area of operations, battlespace, and battlefield organization). Forces are synchronized by commanders by the space,

resources, and action to conduct simultaneous and sequential decisive, shaping and sustaining operations in depth. The outcome of major operations, battles, and engagements are conclusively determined by attacks that are decisive offensive operations. Decisive operations achieve the goals of each phase of a campaign at the operational level. Decisive battles or engagements achieve the purpose of the higher headquarters' mission at the tactical level. Decisive operations are won by commanders through close combat that overcomes the will of the adversary to resist, physically destroys the enemy, or seizes, occupies, and retains location. Effective offensive operations capitalize on relevant information regarding location, weather, and enemy forces and rely very heavily on succinct and accurate intelligence (Offensive Operations 2017b). Information technology (IT) has enabled the military to conduct operations based on more accurate and current information than at any other time in our history, being fully connected to the Command and Control (C2) systems and the information they provide. Commanders can now more effectively synchronize their forces and be more adaptable to the situation at hand or as the situation changes. Subordinates no longer have to wait for directions from headquarters to achieve the intent of their superiors but can more quickly engage and implement with less uncertainty. As one might be able to ascertain from the above, the role of defensive operations cannot be understated in terms of its importance in creating the "right" conditions for commanders to implement their strategies for engaging the enemy. However, the role of offensive operations is undeniably tantamount to bringing the enemy to a position of being defeated or destroyed.

Cyberpower: The Game-Changer

Cyberpower refers to the ability of an environment (cyberspace) to be used for strategic advantage and influence on events in other operational environments and across the instruments of power (Kuehl 2009). Power in cyberspace has provided a different view and perspective from those in the other conventional domains. As noted earlier, the nations that might be classified as the major players in the world during the Cold War era were pretty easy to identify because of two primary yet basic attributes. They were the nations that had very strong military forces and were considered to possess significant economic resources. During this time period, it is also important to note that war was characterized by militaries that were very adept and advanced in their training and possessed a significant cache of conventional weapons. Hence, victory oftentimes came down to strategies, tactics, and operational successes, as well as, considerable economic resources to sustain and empower the nation's military to meet the challenges presented. Indeed, it was not very difficult to recognize the attackers because again there were only a select few that "qualified" or met the limited criteria. In addition, even less were willing to stand up to the challenge of a battle unless there was determined to be no other recourse or options available but to fight. It was more of a matter of being prepared and able to respond to or survive an attack instead of taking on a challenge that the entity was ill-prepared and improperly resourced and trained to address. During this era, as well, it was also

pretty easy to determine where an attack originated and to whom such an attack could be attributed. Time surely could be an issue because major campaigns take time to move major arsenals of conventional weapons and battalions. On some occasions, however, the element of surprise rendered such actions moot or unnecessary because one side was so better prepared and positioned to overwhelm the other side. The aforementioned discussions of war are discussed in the context of the four conventional domains of military engagement, i.e., air, maritime, land, and space.

Cyberspace, as noted in JP 3-12R, is about a global domain framed in an information environment. Libicki reminds us that occasionally one might incorrectly assume cyberspace and information as the same entity. He accurately notes that the two are not identical because a space cannot be defined by a flow of information (Libicki 2009). Libicki also reminds us that the connection of information to warfare is not a new premise for information has always been sought in times of war. Though differences do exist between information and conflict in the kinetic and cyberspace domains, there are some similarities that are important to highlight. For example, in the case of cyberspace and the kinetic domains, situational awareness (SA) strongly influences mission outcome. In addition, cyberspace SA and kinetic SA each contain cognitive biases. Though indeed there are some similarities, there is something undeniably unique about cyberspace that is a significant departure from the four kinetic (conventional) domains. A major difference, however, is that kinetic SA depends strongly upon geography and physical boundaries. Cyberspace SA, on the other hand, is not characterized or defined by geographic boundaries (Kott et al. 2017). Other major differences between cyberspace and the kinetic domains are that in cyberspace the speed (real time or near real time) with which events occur and the inability to clearly determine the source of the attack are major challenges. In the Cold War era, one speaks of a level of "symmetry" between combatants because each had strong military and significant economic resources. There were a number of regions around the world that had one or the other, but few had both.

The challenges previously highlighted in the Cold War era by the few select nation states with strong militaries and economic resources that posed real threats and had to be taken seriously have now evolved to include non-nation state entities. Cyberspace conflicts, which rely on the information environment, have now raised the profile and threat of previously discounted non-state actors because advancements in information and computing technologies have "leveled" and extended the battlefield. Threats are no longer limited to those with large militaries and vast economic resources. Neither are battles fought solely on certain terrains. Cyberspace has provided a level of credibility to non-state actors through technological advancements that have introduced an "asymmetry" in warfare that has created a new set of dynamics that provide non-state actors credibility. It is the intent of cyberspace offensive operations to exploit vulnerabilities in complex information systems that create effects that interfere with the ability of their targets to carry out military or other tasks (Libicki 2012). As conflicts between states and non-state actors become more pervasive, the strategy of asymmetrical warfare has also increased in prevalence.

The Middle East is a classic example of a region in which non-nation states entities are now taken seriously with regards to the threat that they pose to the region's stability. Within the past few decades, asymmetrical warfare has significantly and detrimentally impacted the stability of the Middle East. The region is now faced with a diverse and complicated threat matrix that includes not only the nation-state armies which provided the biggest threats but also now non-state actors who occasionally operate against the nation states. The speed by which weapons can be used in cyberspace, in real-time or near real-time, and the uncertainty in attribution have complicated and delayed retribution, as non-state actors have stepped up their attacks on state assets, including infrastructure. It is important to note that non-nation states not only benefitted from advancements in technology that "leveled the playing field" but also focused on a quick, mobile, and adaptive combatant strategy. This represented a major turn of events in this type of war strategy because the big players clearly were not prepared. Strategies that had worked throughout history were starting to not produce the same kind of results with this new adversary. As noted earlier, the nation states during the Cold War era were very deliberate and methodical in their movements and engagement which took time. As a result, many of the major powers were employing a failed conventional strategy in a cyberspace conflict. The nation states were now the ones being overwhelmed by this new strategic direction which represented a complete paradigm shift in which new speed and agility were the new courses of action.

The asymmetric warfare carried out by non-state actors changed strategy and tactics by becoming more agile, quick, and mobile in their campaigns against the more heavily resourced nation states. The speed afforded by technology advancements allow the smaller non-nation state forces to damage, wear down, and disrupt the activity of the nation state military in the area without confronting it head-on due to relative military inferiority. Unfortunately, the nation states were using conventional battle techniques in a war ill-suited for such a strategy. In terms of military tactics, a number of differences in strategy between the nation and non-nation states became immediately apparent. The nation state organized forces generally fight in an orderly framework while non-state organizations use nontraditional and adaptive methods due to disparities in overt power. Nation states are also less bound by the types of tactics that they use in a conflict because they are less bound by the constraints of international law. National armies, in contrast, have a greater requirement and incentive to operate within international legal limitations due to the limits placed by treaties and diplomatic agreements. Non-state actors are not bound by such agreements. The rise of non-state actors and the use of non-traditional strategies and tactics have altered the nature of conflict in the Middle East. Asymmetrical warfare has similarly been impacted by cyberspace through the broad platform it provides non-state entities to obscure the source of an asymmetric attack. Such an act is possible due to a number of basic characteristics that are unique to cyberspace. First, states for the most part have a broader technological infrastructure and are thus more exposed to attacks in cyberspace than are non-state entities. Second, non-state entities are gaining more access to a wider range of cyberspace capabilities. It is important to examine how society, as a whole, has been impacted.

The Data Explosion and the Impact on the New Information Society

Advancements in information and computing technologies have played a dramatic role in the generation of the massive volumes of data that are entering into people's personal and professional lives. Society has truly transitioned to an information society in which information is used to create some advantage. The volume of data is expanding, annually, in most organizations by 35–50%. Information is being created at an alarming rate being driven by the big data explosion and are processing, annually, more than 60 terabytes (TB) of data – almost 1000 times more than a decade earlier. (Beath et al. 2012). Social media, sensors, mobile technologies, the Internet of Things (IoT) have been major contributors to the massive amounts of data that are now generated. Data itself has evolved in terms of the types that have and will continue to be assessed when technology reaches a certain pinnacle. Though most organizations still focus on structured data in their assessments, semistructured and nonstructured data are gaining more widespread attention in terms of the valuable insight that they can also provide in certain situations. Big data has arrived as the new term-of-the-day as an all-encompassing term that includes structured, semistructured, and nonstructured data. The biggest challenges, to date, are defined primarily in terms of the limits of technology and a lack of qualified data professionals able to address all levels of big data, adequately.

Over time, we have witnessed the evolution of our current society from an agricultural society to an industrial society to currently an information society. Agricultural (agrarian) societies, which go as far back as 10,000 years ago and still exist, were the main form of socioeconomic organizations for most of recorded human history. The agricultural transition identified as the Neolithic revolution has taken place several times over history. Some of the simple correlations between social complexities and the environment disappear in agricultural societies. When less than 50% of the population is directly engaged in agriculture, a transition tends to take agricultural societies into industrial societies. The Industrial Revolution ushered in industrial societies in the late eighteenth century to the present. Advancements in science and technology were largely responsible for the Industrial Revolution. This revolution led to an era of mass production and the division of labor, large increasingly urban populations, significantly higher health, life spans, and standards of living around the world (Wladawsky-Berger 2017). Information societies are driven by the use of information to create advantages. Countries around the world are experiencing the use of information as a catalyst to economic, social, cultural, and political advancements. Information is now recognized as a significant instrument of power. Three main characteristics of an information society are:

- Information is used as an economic resource.
- Possible to identify greater use of information by the public.
- Development of an information sector within the economy.

Often through the improvement of the quality of goods and services they produce, organizations make greater use of information to stimulate innovation, increase efficiency, and increase effectiveness and competition position. In their roles as consumers, people use information more exhaustively to: take better greater control over their own lives; inform their choices between different products; and explore their entitlements to public services. Citizens also use information to exercise their civil rights and responsibilities. The information sector serves the function of satisfying the general demand for information services and facilities. The networks of telecommunications and computers reflect the technological infrastructure that is a significant part of the information sector. However, the information sector is growing faster than the overall economy in nearly all of the information societies. As a result, to keep pace with the growth and demands of an evolving society, there is a need to quicken the development of the Internet content providers (ICPs) – the industry responsible for the information that flows around the networks (Moore 1997). Some of the activities by some of the best known providers of content and information per minute are provided below. For example, per minute

- Facebook users share nearly 2.5 million pieces of content
- Twitter users tweet nearly 300,000 times
- Instagram users post nearly 220,000 new photos
- YouTube users upload 72 h of new video content
- Apple users download nearly 50,000 apps
- Email users send over 200 million messages
- Amazon generates over $80,000 in online sales

It is very important to highlight the role of social media because of the immense impact it has had on data and information flow in such a short period of time. For example, the top two social media platforms in terms of the generation of data per minute are Facebook and Instagram. Facebook, the most active of social networks, generates the most social data, including over 4 million posts every minute. To be exact, that is 4,166,667 which adds up to almost 250 million posts per hour. Second to Facebook is Instagram, whose users (300 million monthly) in 2015 had 1,736,111 likes on photos each minute of the day (~over 100 million likes per hour).

The growth of devices, especially, mobile devices has been a major contributor to the growth in data and information. In terms of sheer mobile usage, however, the mobile web is still in its infancy with much more growth expected. When we add this to the evolution of nontraditional Internet-ready devices with the Internet of Things (IoT), it is uncertain of the heights that might be achieved in the growth of new devices. The Swedish telecom giant Ericsson noted that mobile traffic on data networks has been doubling for the past 2 years since 2013. In 2012, Cisco noted that global traffic on data networks grew by almost 70% in the previous year. By comparison, Cisco gives an indication of how big mobile has become: The traffic on mobile data networks in 2012 – 885 petabytes – was nearly 12 times greater than total Internet traffic around the world in 2000, back when the web was taking off.

Wireless data traffic is expected to continue to grow almost 66% annually to 2018. In other words, by this year, 2017, monthly mobile data traffic should have reached 11.2 exabytes (EB) per month. In 2012, some 4.3 billion people, globally, had mobile devices. This population is expected to come close to a billion by this year or 2018. Annual growth in data traffic will be significantly higher on smartphones (81%) and even higher on tablets (113%). Smartphones, however, will continue to be the biggest consumers of mobile-network data: In 2012, smartphones made up 16% of devices connected to wireless networks and 44% of total traffic. In 2017, they will be 27% of connected devices and consume 68% of data (Kelleher 2013).

Private Sector

Businesses are increasingly recognizing that the key to gaining a competitive advantage depends upon the quality of information available to make those decisions. It is important, however, to interject that it is not about simply acquiring or even possessing the information. It is also about how the information is used in the decision-making process (Jacklic et al. 2011). There is an information revolution that is affecting businesses and their ability to compete in unique ways. For example, the revolution can:

- Alter the rules of competition by changing industry structure
- Provide businesses with new ways to compete, yielding a competitive advantage
- Serve as an "incubator" of new ideas from within or outside of the existing organization that yields new business ventures.

Information, and the technology it requires, is changing the way businesses operate, as well as, how they create and deploy products and services. Increasingly, businesses are recognizing information as a critical resource and asset in their business processes if they are to achieve desired outcomes. The contribution of high quality information to businesses is that it builds confidence in the results, makes it easier to build consensus for major changes in strategy, and provides a competitive edge. In other words, high quality information contributes value to the business. It is hard to talk about the private sector and not include a discussion on value. Specifically, attention should be placed on the value chain which divides a business' activities into distinct economic and technological activities it executes to do business. These distinct activities are called value activities. The value created by a business is measured by the amount that consumers are willing to pay for a product or service. If the value a business creates exceeds the cost of performing the value activities, then the business is profitable. As a result, in order for a company to gain competitive advantage over its competition, it must either generate products or services at a lower cost or perform them in a way that leads to more value – differentiation in quality and cost. Industry has also undergone a transformation by technology in different but no less dramatic ways than the military as it seeks to remain competitive. To remain competitive, companies must cut costs that are associated with how they

obtain, process, analyze, use, and transmit information. In doing so, this has driven dramatic changes in how companies do business.

Differentiated value, which is at the core of competition within the private sector, is not merely about the features of products or services. It is the information about the product or service that has now risen as a priority. Most important is that information creates value very differently than do services or products. For it is surmised that companies that control the information in a process that creates value is optimally positioned to compete and to know where the opportunities lie. In addition, companies that know how to differentiate the way they control the information flow know how to compete and how to win. It is important, however, to note that information (and more importantly, knowledge) is of little benefit if it does not advance desired outcomes. In other words, when information is used to modify future action in beneficial ways, it creates value. Ideally, the learning process will continue as long as the modified future action gives rise to new information (Raynor and Cotteleer 2015).

Somewhat lost in this discussion is the role that information plays to the primary stakeholders in businesses, i.e., shareholders or stockholders. Shareholders hold considerable power as owners of a company, and as owners they have the right to information, e.g., periodic reports on company performance. Basic information such as assets, liabilities, profits, and sales in annual and quarterly reports are required from organizations. However, shareholders and financial analysts more recently have been demanding more comprehensive, understandable, detailed, and frequent information to make more informed decisions. The requests are surely understandable given the accounting scandals of the 2000s. To better position organizations, management must then provide more current, accurate, and not misleading information (Shareholders 2017). Information within the private sector and public domain is primarily used to gain insight and to make decisions for personal or economic gains. It is important to realize that the same information when viewed by different people/groups can lead to different conclusions, as well as, different perceptions of its value. In one case, information may be seen simply as a collection of numbers, whereas, in another case, the same information can be seen as a market opportunity. Next a closer view of citizens and how they view and use information.

Public Domain

The public's interest in information is focused on the satisfaction of personal goals and interests. The word "personal" is emphasized because information connects and empowers people, groups, organizations, communities, and nations. Access to information, though critical, is not the full story. People must understand how to use information to build a better quality of life. When the public feels informed, it can be more willing to share and exchange information with others. Such exchanges, more often than not, better position people to gain the necessary insight needed to make more informed decisions. Unfortunately, it is not always the case that government values two-way information exchanges between itself and the public.

Information is a powerful asset that enables entities to meet goals and objectives as it relates to their needs. It is a much cherished commodity in democratic countries and a much desired one in countries in which information and access are controlled. This is the reason why information is regarded as a very personal commodity and has been the basis for many battles and conflicts throughout the world's history. For example, in India, an ordinary citizen until 2005 had no access to information held by a public authority. Though the constitution of India guaranteed free speech and freedom of expression, a citizen had no legal right to the details of expenditures and public policies. Thus, a common man was unable to scrutinize and observe public actions and understand the outcomes of public activities and/or provide feedback (Ansari 2008). In 2005, the Right to Information (RTI) Act, or the freedom of information or access to information laws, formally defined legislation that "established the general presumption that all information held by the government should be accessible and set out by the mechanisms by which it can be accessed." The "personal" linkage to information is also to connect it to what some in society believe to be a "right" to information as well as a "right" to not have information shared. In particular, the issue of privacy has been a very important one that has surfaced.

Privacy can be defined as "freedom from damaging publicity, public scrutiny, secret surveillance, or unauthorized disclosure of one's data or information, as by a government, corporation, or individual." Privacy has become the subject of much discussion recently because for some there is the feeling that unauthorized access is a violation of their personal space. Technology has dramatically transformed how public information flows and is accessed. Information exchanges and transactions now occur in real-time or near real-time intervals that require a different mindset by the public as how to protect and secure the information. A number of challenging scenarios are possible including: cyber attacks by hackers, unapproved use by a potential government agency, or the freedom given to vendors through memorandums of understanding/agreement (MoU/MoA). One has to now be much more vigilante in terms of what information is available, as well as, limits placed on how the information is used (How to Keep Your Personal Information Secure2017). Personally Identifiable Information (PII) such as health records and financial records are becoming more difficult to protect and secure. Debates continue on the best environments to protect them, e.g., clouds (cloud computing) are believed by some to be more secure, whereas others consider clouds to be more risky.

Proposed Effort and Discussion

The WSIS events of 2003 and 2005 noted earlier represent an excellent example of how the different segments of society can collaborate and come together. Two of the primary pillars of society, confidence, and security are shared by all segments. These pillars provide a motivation for the common lens by which similar outcomes can be achieved. All want to believe that they can pursue and achieve a desired quality of life in a safe environment. However, part of the challenge resides in the ability to identify a "tangible" thread that can require efforts of cooperation and collaboration

to achieve the common ends noted above. The critical infrastructure represents such an entity in the current times. It is defined by the department of homeland security (DHS), as the physical and cyber systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety (Critical Infrastructure 2017). Presidential Policy Directive (PPD) 21 identifies the 16 critical infrastructure sectors in the United States, including: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base (DIB), emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors materials and wastes, transportation systems, and water and wastewater systems (Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience 2013).

About 32 years ago, "infrastructure" was defined in the United States (US) primarily in the context of the adequacy of the nation's public works. The growing threat of international terrorism, however, led policy makers in the mid-1990's to revise the definition of infrastructure in terms of homeland security. To date, there are sixteen (16) critical infrastructure sectors defined with the Department of Homeland Security (DHS) designated as the sector-specific agency for the chemical, commercial facilities, communications, dams, emergency services, energy, government facilities, information technology, nuclear reactors, materials and waste, and co-sector-specific agency for the transportation systems (Critical Infrastructure Sectors 2016). Sector-specific agencies (SSAs) are federal agencies responsible for the protection and resiliency efforts among individual critical infrastructure sectors. The USA PATRIOT Act of 2001 (P.L. 107–56) contains a federal government definition that is often used for "critical infrastructure," i.e., systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validate and Reported to Congress 2013) (H.R.3162: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism 2001). Successive federal government reports, laws, and executive orders have refined, and generally expanded, the number of infrastructure sectors and the types of assets considered to be "critical" for purposes of homeland security. Key decisions must go into how federal agencies make available the services, as well as, protect the information assets of the CI that all of society so heavily depends.

The common, tangible thread that I have chosen is the critical infrastructure, whose value permeates through all segments of society. However, there is still the need to look at common mission in terms that the three communities can coalesce, evaluate, and measure to ensure that goals are met and progress is achieved.

The mission selected is to "protect, secure and enhance critical infrastructure" that to date remains highly vulnerable to attacks. This has become increasingly important as noted earlier because prior to the last 5 or 6 years, there was very little "known" active threats that were actually carried out. As noted in the discussion about the Middle East, this is definitely no longer the case. Infrastructure, specifically critical infrastructure, is now a real and desired target. The goal again is to enable society to

make better decisions about how to optimize resource decisions on the critical infrastructure. To do this the approach that is proposed is to go through four stages called the mission analytics journey. The first stage is to make the mission quantifiable (measureable) – this is often the most difficult step to address because it is hard to know what to measure. This stage follows the premise that specific and challenging goals combined with continual feedback can provide better decisions. Successful approaches have generally followed similar steps, i.e., break down the potential measures in terms of inputs, outputs, and outcomes (Driving Federal Performance 2017; Performance Measurement Strategies and Challenges 2013; Kelkar et al. 2016). Defining mission in quantifiable terms is only the first step. The second step requires the creation of a platform that supports collection, storage, and dissemination of all relevant data. To gain the full picture of mission performance, different datasets may be required to be assembled (Kelly 2015). The third step requires tools to pull the meaning out of the data created in steps 1 and 2. In this step, analytics is used to move data to insight. To do this, three critical questions must be asked that connect operational data to mission outcomes and also separates mission analytics framework from more generic business intelligence tools. The three critical questions are: What? So What? and What if? The last step is to understand that insights without action have very little value. In step 4, insights are translated into actions (Goldsmith 2013).

In this study, I was drawn to the use of the Office of Management and Budget (OMB) Program Assessment Rating Tool (PART) because it recognizes the challenges of developing suitable measures and focuses on end outcomes (Gilmour 2007). In addition, it allows for measures relevant for partners outside of the government, i.e., the private and public sectors. Outside contributions are critical because the critical infrastructure is almost 90% owned by the private sector and needs to incorporate issues relevant to the private sector and citizens. Though OMB's focus is on the performance of an agency program (in this case the Critical Infrastructure program which falls under DHS), it also has 25–30 questions grouped according to four categories that enable contributions from all of the segments. Rarely, if at all has an assessment considered the critical infrastructure in the context of all three segments of society. The public sectors' relationship has largely been confined to the services that are provided.

The PART focuses on the four major areas listed below. Each of the answers to the questions is given a weighted score for relative significance, including:

1. Program Purpose and Design (weight = 20%): Program design and purpose are clear and defensible.
2. Strategic Planning (weight = 10%): Agency sets valid annual and long-term goals for the program.
3. Program Management (weight = 20%): Agency management of program, including financial oversight and program improvement efforts.
4. Program Results (weight = 50%).

For example for the Critical Infrastructure program run by DHS, the Table 1 provides an example of possible inputs, outputs, and outcomes for the government, private, and public sectors.

Table 1 Inputs, outputs, and outcomes for PART tool for critical infrastructure

Measures	Government	Private sector	Public sector
Inputs: Factors such as resources or funding	Grants, fees, appropriations, cooperative agreements	Investments (shareholders), fees	Fees
Outputs: Products of the government activity itself (may be less directly relevant to citizens)	Improved information sharing with the private sector, more consumer and industry-friendly policies	More responsiveness and information sharing	N/A
Outcomes: The consequences of direct relevance to citizens and equates most closely to actual mission goals	Public satisfaction, better coordination and equitable partnership with private sector	Improved information sharing, collaboration and cooperation	Efficient and cost-effective services

The quantitative scores are then converted to grades that enable an observer to determine first hand if there are gaps and where those gaps can be addressed to meet infrastructure requirements and performance expectations.

Conclusion

Mission, culture, stakeholders, shareholders, priorities, and desired outcomes play a major role in defining and distinguishing the three segments of society. The military defines offensive operations in terms of an outcome of defeating or destroying an enemy. For the public and private sectors offense can be viewed in terms of personal goals. The private sectors use of offensive operations could be defined in terms of outcomes that lead to increased shareholder value and market share. For the public, offensive operations could be defined in terms of an outcome that leads to a better quality of life. The differences between the different communities can at times seem too wide to overcome. However, all of society shares the common desire for a secure and unobstructed existence. The key is to find a shared and common outcome that compels the three segments of society to see the world through a similar lens. The critical infrastructure (CI) represents such a common and shared thread that affects all segments of society. It is a complex and dynamic "system of systems" with intrinsically linked components that act as vital "arteries" to services that enable society as a whole to function. The critical infrastructure, considered relatively safe in the past, has now become a viable and prized target vector for attack. Advancements in technology, difficulty in attribution, potential impact of attack, and a lack of responsiveness of organizations to cyber threats and vulnerabilities have even more emboldened perpetrators to aggressively pursue attacks.

A disconnect based on some of the aforementioned factors have driven wedges of mistrust and complacency between the three sectors in such a way that the critical information sharing and responsiveness needed to secure and generate a more

efficient and cost-effective critical infrastructure continues to be elusive. This effort proposes that offensive operations, as we know them for the military/DoD, be redefined in terms of a new offensive paradigm that promotes a more data-driven collaboration that is shared between the three segments of society. The goal is to develop in terms of real measures a quantifiable mission that can mitigate many of the factors that have challenged the ability to achieve optimal security and performance of the critical infrastructure sectors. Future efforts will examine more fully the scoring of the PART on the inputs, outputs, and outcomes and translate numerics to grades. In addition, once the mission has been quantified, the other steps in the mission analytics journey will be completed. The next effort will also focus on a select critical infrastructure sector to enable more details to be collected and then will seek extend the effort to other sectors. The Analytic Hierarchy Process (AHP) will be used also to define quantitatively important parameters and specifices to the critical infrastructure sector. In particular, the Analytic Hierarchy Process (AHP) will be used to translate the scoring variables, e.g., inputs, outputs, and outcomes enlisted by the OMB PART into decision parameters that better enable senior leaders to make more informed decisions which ensure that resources and information assets are securely operated and available to meet mission needs and objectives. The next effort will also focus on a select critical infrastructure sector (i.e., the electric power or utilities sector) to reveal more detailed and specific results that reflect how the resources operate optimally, while being secured against terrorist and cyber attacks. The intent will also be to then extend the work to other critical infrastructure sectors.

References

Ansari, A. (2008). Right to information and its relationship to good governance and development. http://www.nfici.org/attachments/article/163/IC-MA-LectureAtUNESCO-04122008.pdf. Accessed 10 February 2017.

Beath, C., Becerra-Fernandez, I., Ross, J., & Short, J. (2012). Finding value in the information explosion. *MIT Sloan Management Review*, 17–21.

Berners-Lee, T. (2017). History of the web. Retrieved from World Wide Web Foundation: http://webfoundation.org/about/vision/history-of-the-web/. Accessed 10 February 2017.

Challenges for the Intelligence Community. (2011). In B. Fischoff, H. Arkes, B. Buendo de Misquita and T. Fingar, Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences (pp 5–21). Washington, DC: National Academies Press.

Critical Infrastructure. (2017). Retrieved from Department of Homeland Security: https://search.dhs.gov/search?query=critical+infrastructure&op=Search&affiliate=dhs. Accessed 10 Feb 2017.

Critical Infrastructure Protection: DHS list of priority assets needs to be validate and reported to congress. (2013).Washington, DC: GAO-13-296. Accessed 10 Feb 2017.

Critical Infrastructure Sectors. (2016) Retrieved from Homeland Security: https://www.dhs.gov/critical-infrastructure-sectors. Accessed Feb 10 2017.

Cyberspace Operations. (2013). Retrieved from Joint Publication 3–12 (R): http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

Defensive Operations. (2017). Retrieved from GlobalSecurity.org: http://www.globalsecurity.org/military/library/policy/army/fm/3-0/ch8.htm

Driving Federal Performance. (2017). Retrieved from Performance.gov: https://www.performance.gov. Accessed 10 Feb 2017.

Gibson, W. (1984). *Neuromancer*. New York: Ace Books.
Gilmour, J. (2007). Implementing OMB's program assessment rating tool (PART): Meeting the challenges of integrating budget and performance. *OECD Journal on Budgeting*, 1–40.
Goldsmith, S. (2013). *How Louisville, Ky is using a stat program to transform the culture of government*. Retrieved from Governing: http://www.governing.com/blogs/bfc/col-efficiency-louisville-louiestat-performance-metrics-improvement-transform-government-culture.html. Accessed 10 Feb 2017.
H.R.3162: Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism. (2001). Retrieved from Congress.gov: https://www.congress.gov/bill/107th-congress/house-bill/03162. Accessed 10 Feb 2017.
How to Keep Your Personal Information Secure. (2017). Retrieved from Consumer Information: https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure. Accessed 10 Feb 2017.
Jacklic, J., Popovic, A., & Coelho, P. (2011). *The impact of quality information provided by business intelligence systems on the use of information in business processes* (pp. 158–167). Berlin/Heidelberg: Springer.
JFODS4: The Joint Forces Operations & Doctrine SMARTbook. (2015). In N. Wade (Ed.), *About the instruments of national power (a whole of government approach)*. Totowa: The Lightning Press.
JP 1: Doctrine for the Armed Forces of the United States. (2013). Retrieved from Lightning Press: http://www.dtic.mil/doctrine/new_pubs/jp1.pdf. Accessed 10 Feb 2017.
Kelkar, M., Viechnicki, P., Conlin, S., Frey, R., & Strickland, F. (2016). *Mission analytics: Data-driven decision making in the government*. New York City: Deloitte.
Kelleher, K. (2013). *Mobile growth is about to be staggering*. Washington, DC: Fortune.
Kelly, E. (2015). *Introduction: Business ecosystems come of age*. New York: Deloitte University Press.
Kott, A., Buchler, N., & Schaefer, K. (2017). Kinetic and cyber. Retrieved from Arxiv.org: https://arxiv.org/ftp/arxiv/papers/1511/1511.03531.pdf. Accessed 10 Feb 2017.
Kuehl, D. (2009). From cyberspace to cyberpower: Defining the problem. In F. Kramer, S. Starr, & L. Wentz (Eds.), *Cyberpower and national security* (pp. 37–40). Washington, DC: National Defense University Press.
Leiner, B. M., Cerf, V. G., Clark, D., Kahn, R. E., Kleinrock, L., Lynch, D., . . . & Wolf, S. (2017). The brief history of the Internet. Retrieved from Internet Society: https://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet. Accessed 10 Feb 2017.
Libicki, M. (2009). Military cyberpower. In F. Kramer, S. Starr, & L. Wentz (Eds.), *Cyberpower and national security* (pp. 275–284). Washington, DC: National Defense University Press.
Libicki, M. (2012). Cyberspace is not a warfighting domain. *I/S: A Journal of Law and Policy for the Information Society*, 321–336.
Military power potential. (2017). Retrieved from Encyclopedia.com: http://www.encyclopedia.com/social-sciences/applied-and-social-sciences-magazines/military-power-potential#C. Accessed 10 Feb 2017.
Moore, N. (1997). *The information society.* Paris: UNESCO.
Nichiporuk, B. (2002). U.S. military opportunities: Information warfare concepts of operation. In Z. Khalilzad & J. Shapiro (Eds.), *Strategic appraisal: U.S. air and space power in the 21st century* (pp. 187–223). Arlington: Rand. Retrieved from https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1314/MR1314.ch6.pdf. Accessed 10 Feb 2017.
Offensive operations. (2017b). Retrieved from GlobalSecurity.org: http://www.globalsecurity.org/military/library/policy/army/fm/3-0/ch7.htm#par8. Accessed 10 Feb 2017.
Performance measurement strategies and challenges. (2013). Retrieved from Office of Management and Budget: https://www.whitehouse.gov/sites/default/files/omb/part/challenges_strategies.pdf. Accessed 10 Feb 2017.
Power. (2017). Retrieved from Dictionary.com: http://www.dictionary.com/browse/power. Accessed 10 Feb 2017.
Presidential Policy Directive (PPD) 21: Critical infrastructure security and resilience. (2013). Retrieved from Office of the White House: https://fas.org/irp/offdocs/ppd/ppd-21.pdf. Accessed 10 Feb 2017.

Quick, C. (2014). *Cyberspace as a weapons system*. Arlington: Landpower Publication.
Raynor, M., & Cotteleer, M. (2015). The more things change:Value creation, value capture, and the internet of things. *Deloitte Review*, 1–17.
Shareholders. (2017). Retrieved from Reference for Business: http://www.referenceforbusiness.com/index.html. Accessed 10 February 2017.
Weapons. (2017). Retrieved from Miltary.com: http://www.military.com/equipment/weapons. Accessed 10 Feb 2017.
Whitehead, Y. (1999). Information as a weapons: Reality vs Promises. Retrieved from Iwar.org: http://7.iwar.org.uk/iwar/resources/usaf/maxwell/students/1997/whitehead-update.pdf. Accessed 10 Feb 2017.
Wladawsky-Berger, I. (2017). Reflections on the transition to an information society. Retrieved from Irving Wladawsky-Berger: http://blog.irvingwb.com/blog/2011/05/reflections-on-the-transition-to-an-information-based-society.html. Accessed 10 Feb 2017.
WSIS+10: WSIS Review Process. (2005). Retrieved from World Summit on the Information Society: https://www.itu.int/net/wsis/review/2003-2005.html. Accessed 10 Feb 2017.

IP Hopping by Mobile IPv6

46

Vahid Heydari

Contents

Abstract

Remote cyberattacks can be started from unlimited distance. These remote attacks include special actions which allow attackers to compromise remote systems.

V. Heydari (✉)
Department of Computer Science, Rowan University, Glassboro, NJ, USA
e-mail: heydari@rowan.edu

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_49

During the first step of attacks, reconnaissance step, attackers attempt to gather information about their intended target(s). For network-based systems, figuring out the IP address(es) of the target(s) is critical to the success of the attack. There are several countermeasures to protect systems from these attacks such as firewalls and intrusion detection and prevention systems (IDPS). Unfortunately, zero-day exploits that use undisclosed or uncorrected computer application vulnerabilities can defeat the best firewalls and IDPSs. Regardless of the strength of these countermeasures used in practice, the use of static IP addresses leaves the target vulnerable in two ways. First, they are discoverable. Second, after accessing the target, the attacker can maintain this access for a long time. So, an effective defense is a mechanism to change the IP addresses randomly and dynamically (IP hopping). These mechanisms are called moving target defenses (MTDs). In this chapter, some novel methods based on IPv6 (and Mobile IPv6) are explained to thwart remote attacks by randomly changing the IP address(es) of the target(s).

Keywords

Address-based DDoS attack · Attack handling · Authentication header (AH) · Binding identification (BID) · Binding update list (BUL) · Deception · Deterrence · Distributed denial-of-service (DDoS) · Dynamic host configuration protocol (DHCP) · Dynamic interface IDentifier (IID) · Encapsulating security payload (ESP) · Home address option (HAO) · Intrusion kill chain · Intrusion prevention and detection systems (IPDS) · IP hopping MTD · IP security (IPsec) · Mobile IPv6 · Moving target defense (MTD) · Moving target IPv6 defense (MT6D) · Moving target mobile IPv6 defense (MTM6D) · MVPN · OpenFlow random host mutation (OF-RHM) · Route advertisements (RAs) · Routing header type 2 (RH2) · Secure shell (SSH) · SLAAC mechanism · Stateless address autoconfiguration (SLAAC) · Trusted dynAmic logical hEterogeNeity sysTem (TALENT) · Virtual machine live migrations (VM-LM)

Introduction

Remote attackers are always looking to find vulnerabilities of their intended target (s). Toward this goal, the attackers use different ways to compromise remote systems. Knowing Internet Protocol (IP) addresses of targets is the main requirement for address-based remote attacks. The address-based remote attacks include two main categories: (1) address-based distributed denial-of-service (DDoS) and (2) remote exploits.

Address-based DDoS attack uses multiple compromised systems to target a single victim computer. However, for remote exploits, one computer can be used by an attacker to gain unauthorized access to a vulnerable victim. To start remote exploit attacks, vulnerabilities should be found on the victims. For example, an attacker can use remote code execution vulnerability to execute malicious codes and obtain a remote access to a victim. The attacker can also use privilege escalation vulnerability

to gain more privileges on the victim. In this case, the victim is compromised and may also be used for attacking other computers.

To prevent these attacks, we need to know the attack process and each step taken by attackers. Once we understand the steps of a successful attack, then we may be able to detect or mitigate the attack. Intrusion kill chain (Hutchins et al. 2011) is a systematic process that outlines these steps. This end-to-end process is described as a chain because failure of each step will break entire process. The steps of the intrusion kill chain is defined as (1) reconnaissance, (2) weaponization, (3) delivery, (4) exploitation, (5) installation, (6) command and control, and (7) actions on objectives. The best advice for defenders is moving their detection and prevention measures up the kill chain to reduce the cost and damage caused by any attack.

During the first step of an attack (reconnaissance), an attacker needs to gather information about its target. The first required information is the target's IP address. When the attacker finds the IP address of the target, the attacker will be able to scan the target's open ports and services. For example, a target with an enabled remote access service such as Secure Shell (SSH) could be a good choice for the attacker. In this case, the attacker can send one connection request to the target to receive the SSH server string. This string reveals which SSH implementation (version number) is used on the target. If the version of the SSH implementation is not up-to-date, then the attacker does not need to write any piece of code. In fact, some exploit codes could be found based on the service and its old version number. Using one of those exploit codes makes the attacker able to obtain remote access to the target.

There are several countermeasures to protect systems from the attacks discussed above. These countermeasures include firewalls and intrusion prevention and detection systems (IPDS). Regardless of the strength of these countermeasures used in practice, preventing attackers to gather information about targets, i.e., attack surfaces (Manadhata and Wing 2011), could be the best way to combat remote attacks. The use of static IP addresses leaves the target vulnerable because they are discoverable and after the victim is found, the attacker has enough time to discover a penetration way in order to gain access to the target. Dynamic IP addressing (IP hopping), on the other hand, can change the target's IP address randomly and dynamically. More specifically, it can limit the amount of time the attacker has to find the target. In fact, the attacker has to constantly try to find the target's IP address. This type of defense mechanism is called the moving target defense (MTD). The goals of IP hopping MTD are as follows:

- Deter: Ability to increase attackers' level of effort needed to achieve their goals. Deterrence is the most effective way to secure a system from cyberattacks. It increases the cost of malicious activity because of increase in the resources required by attackers. This goal can be achieved by IP hopping because of using random IP addresses.
- Deception: Ability to increase uncertainty and apparent complexity for attackers. IP hopping can deceive attackers by dynamically changing the IP address of the target.

  In order for this strategy to work, some challenges have to be overcome:

- Selecting the next random IP address of the system should be highly unpredictable.
- Changing the IP address should be done in a short interval.
- Changing the IP address should not cause any unavailability of the system for legitimate peers.
- Implementation of this method should not need any change in the network equipment.

In this chapter, some novel IPv6 (and Mobile IPv6)-based moving target defense are explained. This chapter starts by some background material (see section "Background") and continuous with related work (see section "Related Work"). Next, three new methods, MT6D (see section "MT6D"), MTM6D (see section "MTM6D"), and MVPN (see section "MVPN"), are explained. Finally, some conclusions are offered in section "Conclusion."

Background

In this section, stateless address autoconfiguration, Mobile IPv6, route optimization, return routability procedure, binding management, multiple Care-of addresses, and communication by IPsec are introduced. These concepts are essential for understanding the rest of the chapter.

Stateless Address Autoconfiguration

Dynamic Host Configuration Protocol (DHCP) (Droms et al. 2003) is a way to automatically assigns hosts' IP addresses. Stateless address autoconfiguration (SLAAC) (Thomson et al. 2007) is another way for easier configuration of IPv6 addresses. SLAAC helps hosts to automatically generate global IPv6 addresses without needing any help of DHCP servers. For this purpose, hosts should use router discovery message of Neighbor Discovery protocol (Narten et al. 2007) via the Internet Control Message Protocol version 6 (ICMPv6) (Conta et al. 2006).

With SLAAC, routers periodically send route advertisements (RAs) via ICMPv6. Each RA message includes information about its subnet like its router's prefix (the first 64 bits of the IPv6 address). If a host is configured to use SLAAC to obtain its IPv6 address, the host listens for the RA message and takes the advertised prefix to generate a unique IPv6 address. For this strategy to work, SLAAC dynamically generates a host identifier that is 64 bits (based on the host's MAC address by default) and combines it with the advertised prefix (64 bits) to create a 128-bit IPv6 address (tentative address). This generated address should be checked against current occupancy. For this goal, a neighbor solicitation message is sent with the tentative address as the destination address. If someone else has the same address, it will send back a neighbor advertisement message. In this case, the host cannot use this tentative address and should generate another address to finally find an

unoccupied IPv6 address. After that, the final address will be used as the global IPv6 address of the host.

SLAAC mechanism makes a host able to dynamically change its IPv6 address. Because of this valuable mechanism, IPv6 has been used as the base of new generations of IP hopping methods.

Mobile IPv6

To provide mobility function to IP devices, Mobile IPv6 was standardized in 2004 (Johnson et al. 2004). The latest revision of Mobile IPv6 was published as RFC 6275 in 2011 (Perkins et al. 2011). A host which supports the Mobile IPv6 protocol can move from one subnet to another. It means the host can change its point of attachment to the Internet. The IP address of each host is assigned based on the prefix address of its current subnet. Therefore, when the mobile node (MN) moves from one subnet to another, its previous IPv6 address becomes invalid in the new subnet. To solve this problem, Mobile IPv6 uses a second IP address.

Handling the changing IP address of an MN is one of the most important features of Mobile IPv6. For this goal, an MN in Mobile IPv6 has two types of IPv6 addresses:

- Permanent IP address: Home address (HoA) is assigned to the MN when it is attached to its Home agent (HA). HA is a router in the home network that acts like a proxy for the MN.
- Current IP address: Care-of address (CoA) is assigned to the MN when it moves to a foreign network.

At the beginning, the MN is attached to its HA and registers its HoA on the HA. When the MN moved to a foreign network, it registers a CoA based on the prefix address of that network. Then, the MN updates its HA with its new CoA. For this goal, the MN sends a message called binding update (BU) to the HA. The BU message includes both CoA and HoA (binding information) of the MN.

When the HA receives the BU message and accepts it, the HA sends a binding acknowledgement (BA) message to confirm that the BU message is accepted. Then, a bidirectional tunnel is created between the IP address of the HA and the MN's CoA. After this step, all packets with the MN's HoA on their destination address are intercepted by the HA and tunneled to the MN. The tunnel is also used to send packets originated at the MN to correspondent nodes (CNs). This process is shown in Fig. 1.

Communication path between the MN and its CN via the tunnel may be longer than direct path between them. For example, if the MN moves to the CN's subnet, they should still use the HA for packet exchanging. This situation called triangular routing was one of the major problems of Mobile IPv4 (Perkins 2010). Route optimization mechanism is the solution used by Mobile IPv6 for direct communication between the MN and a CN.

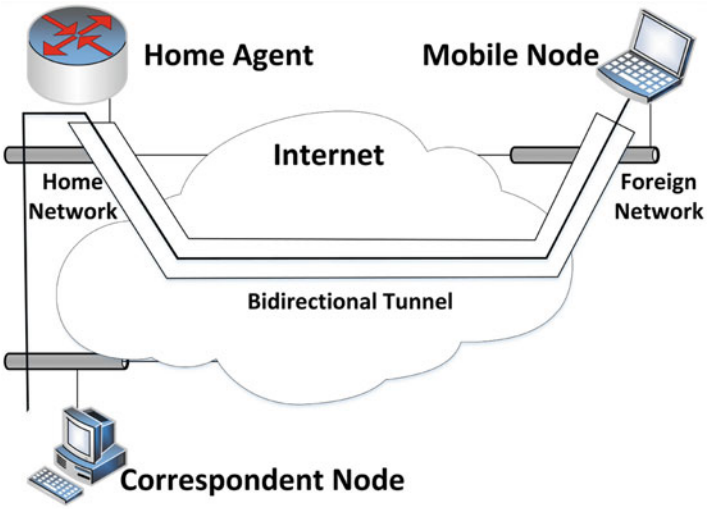


Fig. 1 Mobile IPv6 bidirectional tunnel

Route Optimization

Route optimization mechanism is a part of Mobile IPv6 standard. This mechanism is used to forward packets between an MN and its peer node (CN) via a direct path without detouring through the MN's HA. In order for this strategy to work, both the MN and the CN should support the route optimization mechanism according to the specification of Mobile IPv6.

To optimize the route, the CN should hold the current CoA of the MN. Therefore, when the MN moves to a new subnet, the MN should send a BU message to the CN. This BU message includes the latest CoA of the MN. After the successful route optimization mechanism, the MN and the CN will have a direct communication path as illustrated in Fig. 2. In fact, the source IP address of each packet's header originated at the MN is the CoA. The same CoA is also used as the destination IP address of each packet's header originated at the CN. Therefore, different IP addresses (CoAs) are used in packets' header depending on the current position of the MN. However, changing IP addresses of peer nodes causes communication disruptions in the upper layers (e.g., TCP sessions). To make it transparent to the upper layer, the permanent IP address (HoA) of the MN should be used in the upper layer. Therefore, the HoA needs to be swapped with the CoA in the source. The HoA is also needed to be stored in packets' header and swapped with the CoA in the destination. For this purpose, Mobile IPv6 defines a new extension header called routing header type 2 (RH2) and a new option called home address option (HAO) as a part of destination option header of IPv6 (Deering and Hinden 1998).

The routing header type 2 is used to carry an MN's CoA in packets originated at an HA or a CN to the MN. After the route optimization mechanism, the CN stores the

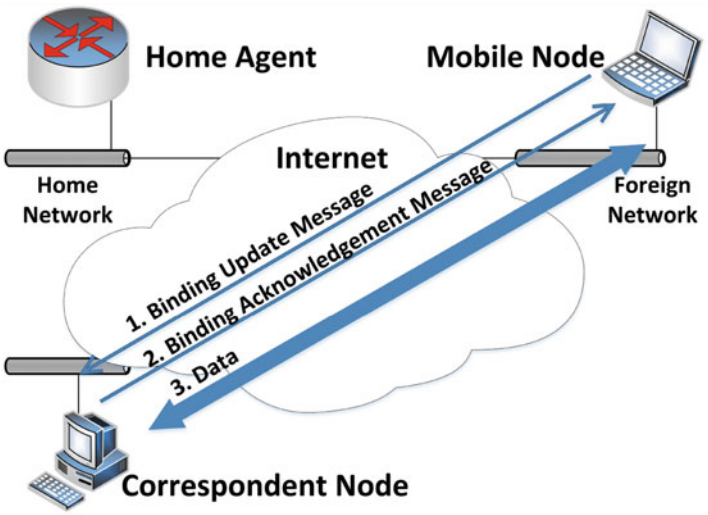


Fig. 2 Optimized communication between an MN and a CN

MN's HoA in the routing header type 2 of each packet's header and uses the MN's CoA as the destination IP address and forwards the packet. Therefore, the packet is sent directly to the MN's CoA. When the MN receives this packet, the MN swaps the address stored in the routing header type 2 (HoA) with the destination IP address of the packet (CoA). Then this packet is forwarded to the upper layers. In this way, upper layer protocols of both the MN and the CN always see permanent IP addresses of the peer nodes.

The destination options header is used to carry optional information that needs to be processed only by destination nodes. The home address option, as a part of the destination option header, stores the MN's HoA in each packet's header when the packet is sent by the MN while away from the home network. In this case, the MN's CoA is stored in the source IP address of the packet. When the CN receives the packet, the CN swaps the source IP address of the packet (CoA) with the HoA stored in the home address option. Note that the CN checks its binding cache (explained in section "Binding Management") before swapping the addresses.

Return Routability Procedure

Protecting BU messages is very important in the route optimization mechanism. If a CN accepts a BU message without any verification, an attacker is able to redirect packets sent to the MN to the attacker. Therefore, a BU message should be protected by return routability procedure (Perkins et al. 2011). This procedure creates a shared secret between an MN and a CN. The procedure provides a method to prove to the CN that the CoA and HoA included in the BU message are owned by the MN.

Before sending a BU message, the MN sends two messages: one of them is sent with its HoA in the source address of the message called home test init message and another one with its CoA called care-of test init message. The CN receives the first message through the MN's HA and the second message through a direct path. The CN replies to both messages with a home test message and care-of test message, respectively. The home test and care-of test messages include token values computed by the CN. When the MN receives these replay messages, the MN generates a shared secret using the token values and puts it in the BU message. The CN can verify the BU message based on the sent token values to make sure that the MN has received both home test and care-of test messages. That means the HoA and the CoA of the BU message are assigned to the same MN.

Each time the MN changes its CoA, the same procedure is needed to verify the right of the MN to use the HoA and the validity of its CoA. The return routability procedure adds some overhead and delay to the route optimization mechanism because of adding four extra messages per each BU message.

Binding Management

Binding update list (BUL) and binding cache (Perkins et al. 2011) are two data structures used for optimizing the route between an MN and a CN based on the route optimization mechanism. Each MN has a BUL and each CN has a binding cache.

The BUL stores information per each BU message sent by the MN to its CNs. When the MN wants to send a BU message to a destination that has already received the previous BU message, the MN updates the related BUL entry with this new BU message. When the MN changes its CoA, it automatically sends BU messages to all of its CNs found in the BUL.

The MN checks the BUL before sending each data packets. If the destination of the packet is found in the BUL, the packet should be sent using direct path by inserting the CoA as the source address in the header of the packet and HoA in the home address option. Each BUL entry includes some information like:

- The IP address of a CN to which a BU message was sent
- The HoA for which the BU message was sent
- The CoA that is sent in the BU message

The binding cache of a CN includes binding information of an MN received by the CN. When the CN receives and verifies a BU message, the CN inserts an entry in the binding cache or update it. The entry includes some fields like:

- The HoA of the MN for which this is the binding cache entry
- The CoA of the MN obtained from the BU message

When the CN has a data packet to send, the CN checks the binding cache for the destination address of the packet. If the destination address of the packet is found as

the HoA of an MN, the CN puts the related CoA of the MN in the destination address in the packet header and the HoA in the routing header type 2.

The binding cache is also checked when the CN received a packet with the home address option. If the entry is found, then the CN swaps the source address and the HoA of the packet header.

Multiple Care-of Addresses

The binding identification (BID) number extension of the Mobile IPv6 standard can be used by an MN to utilize multiple CoAs over the same HoA with its CNs (Wakikawa et al. 2009). In this way, the MN can register multiple IPv6 addresses as its CoAs. For this purpose, the MN generates a unique BID per each CoA and stores these BIDs in the BUL. The BIDs are used to handle each binding independently. BU messages via the binding identifier mobility option are used to register the MN's CoAs.

If the multiple care-of addresses registration is disabled on the CNs, they cannot understand the BID mobility option included in the BU messages. Therefore, this unknown mobility option is ignored by the CNs. As the result, each CN will put the new received CoA in the binding cache and use it to send packets to the MN. This process helps the MN to have a unique CoA per each CN or per each group of CNs.

Communication by IPsec

IP security (IPsec) is a set of mechanisms to protect IP communications. Supporting IPsec was originally a mandatory requirement of IPv6 but RFC 6434 (Jankiewicz et al. 2011) made it only a recommendation. The base architecture to implement and deploy IPsec is described in Kent and Seo (2005). IPsec provides the following security features for each IP packet of a communication session:

- Authentication: verifies that the received packet is actually from the claimed sender
- Integrity: ensures that the packets' contents did not change in transit
- Confidentiality: conceals the packets content through encryption

Two main protocols used by IPsec are as follows:

- Authentication header (AH): provides data origin authentication and data integrity (Kent 2005a)
- Encapsulating security payload (ESP): provides confidentiality, data origin authentication, and data integrity (Kent 2005b). Using IPsec ESP is recommended In Mobile IPv6 (Perkins et al. 2011).

When a packet is ready to be sent by an MN, the packet has already supplied the HoA as the source address in its header. If a BUL entry is found for the destination of

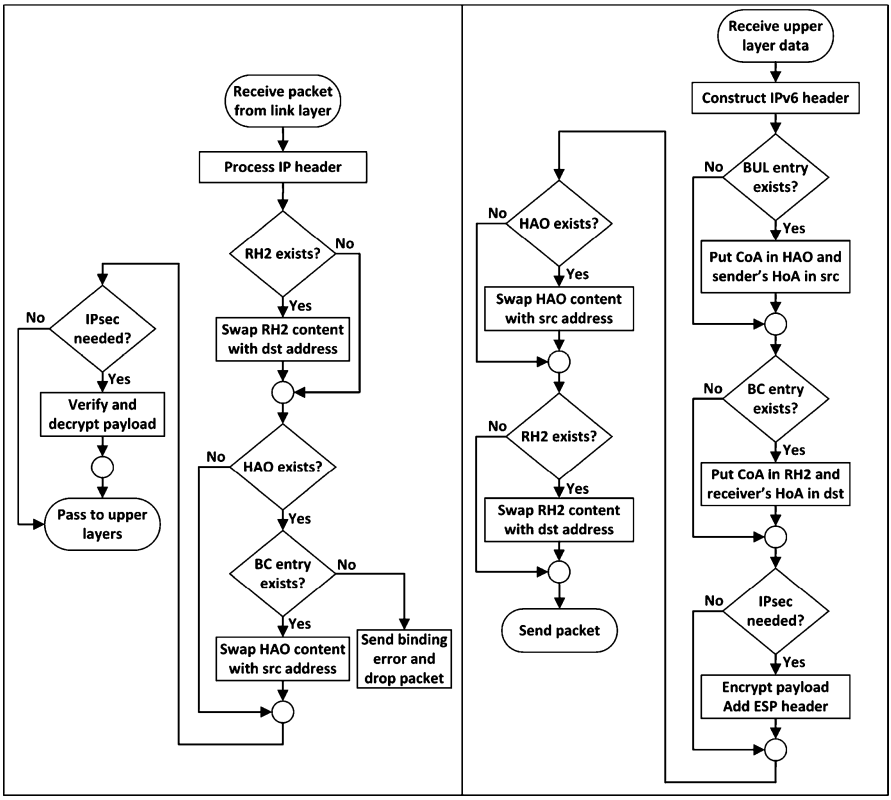


Fig. 3 Packet processing: (*left*) received packets' processing flowchart (*right*) sending packets' processing flowchart

this packet, the MN extracts the CoA of the entry and inserts it in the home address option of the packet.

When the packet reaches IPsec, it will be encrypted and some headers will be added. After that, the home address option (CoA) is swapped with the source address (HoA) of the packet header.

When the CN receives this packet, the home address option and the source address will be swapped. Then, the IPsec implementation receives the packet. Therefore, when the packet is processing by IPsec, the HoA is in the source address of the packet. Because of this process, the HoA is used by IPsec as the selector to avoid changing the security association per each updated CoA of the MN. These processes are shown in Fig. 3.

According to this standard Mobile IPv6 and IPsec implementations, the source or the destination address header of a packet on the path is the MN's CoA. Note that the MN's HoA is still in the packet header in the routing header type 2 or the home address option as illustrated in Figs. 4 and 5.

Fig. 4 Packet format with RH2 (CN to MN)

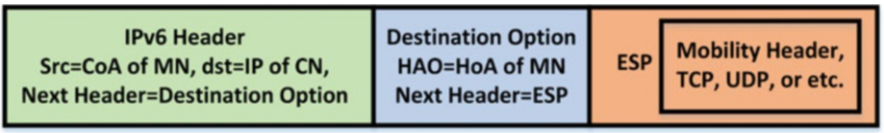


Fig. 5 Packet format with HAO (MN to CN)

Related Work

This section includes a brief review of some remote attack protection methods based on MTD. Also, some of the limitations of these methods are discussed.

Some cloud-based MTD methods were presented in Stavrou et al. (2005), Wang et al. (2014), and Jia et al. (2014) to combat DDoS attacks against Internet services. In these methods, selective server replication and intelligent client reassignment are used on the victimized servers. These servers are turned into moving target in order to isolate attacks. When a server is under attack, the server instance is replaced with a new replica at another network location. Then, the clients are migrated to this new replica of the server. In order for this strategy to work, only migrated clients know the new location of the server. When the clients' migration is completed, the victimized server is recycled.

Another group of cloud-based MTD methods are based on virtual machine live migrations (VM-LM). These methods focused on integrity of software before migration (Danev et al. 2011) or considered the availability and duration of migration in practice (Zhang et al. 2012).

Trusted dynAmic Logical hEterogeNeity sysTem (TALENT) (Okhravi et al. 2012) is a method designed for critical infrastructure applications. It is a framework for migrating mission critical applications to a different platform at random time intervals when an attack or new vulnerability is discovered. Based on the live-migration of the TALENT method, changing the hardware and operation system on top of which a sensitive application is running will be possible. In this method, the state of the application (execution state of the process and its open files and sockets) is preserved during the migration. More specifically, TALENT creates a moving target by changing the platform on-the-fly.

A hierarchical attack representation model is presented in Hong and Kim (2016) to assess the effectiveness of these cloud-based MTD methods. A formal security analysis with various performance and security metrics was leveraged for this comparison.

The above-mentioned MTD methods do not aid in prevention. More specifically, these methods are reactive in nature. Furthermore, detecting flooding attacks could be possible through the use of state-of-the-art tools and techniques in network traffic analysis (Gil and Poletto 2001; Hussain et al. 2003). However, it is not easy to detect penetration attacks such as remote exploits that take advantage of target vulnerabilities. Detecting zero-day vulnerabilities, previously unseen vulnerabilities, are even more difficult to detect. Therefore, considering both prevention and treatment measures in place is desirable to provide better security overall.

OpenFlow random host mutation (OF-RHM) is an MTD method introduced in Jafarian et al. (2012). The goal of this method is changing IP addresses of end-hosts randomly, frequently, and quickly using software-defined networking (SDN) approach. SDN provides flexible infrastructure in order to develop and manage random IP addresses. In this method, Real IP address (rIP) of each host remains unchanged but a new virtual IP (vIP), selected from the unused network address space, is assigned to each host at regular intervals. vIPs will be used as the only routable addresses and are automatically translated into the rIPs and vice versa at the network edges close to the source or destination host. Implementation of this method requires two major components: (1) gateways to perform rIP-vIP translation by OpenFlow switches and (2) a central management authority by a centralized controller (Gude et al. 2008). For scalability, several controllers can be used that each one should manage a segment of the network. After initialization, no information need to be exchanged among controllers; therefore, each controller can act independently.

OpenFlow has some advantages such as being transparent to the end hosts (does not need any change in the end hosts' hardware or software) and not using any type of encapsulation for data packets. On the other hand, drawbacks of this method are requiring central authority management (NOX controller) and new equipment (OpenFlow switches).

MT6D

Moving target IPv6 defense (MT6D) (Dunlop et al. 2011) is one the best prevention methods that leverages the huge address space of IPv6. MT6D is designed to achieve two goals: (1) protecting against targeted network attacks and (2) maintaining user privacy. MT6D repeatedly changes the IP addresses of both peer hosts midsession without dropping sessions to prevent attackers who want to discover the identities of the peer hosts. In order for this strategy to work, IPv6 is used because of the ability to seamlessly bind new IP addresses via SLAAC.

Changing IP addresses midsession can also prevent attackers to determine that the same two hosts are communicating. Furthermore, attackers need to reacquire their targets after each rotation interval (Fig. 6).

Dynamically rotating the IP addresses of the peer hosts helps MT6D to prevent some attacks such as address-based DoS (or DDoS) and man-in-the-middle (MITM) attacks. These attacks can be started by obtaining the IP addresses of their targets

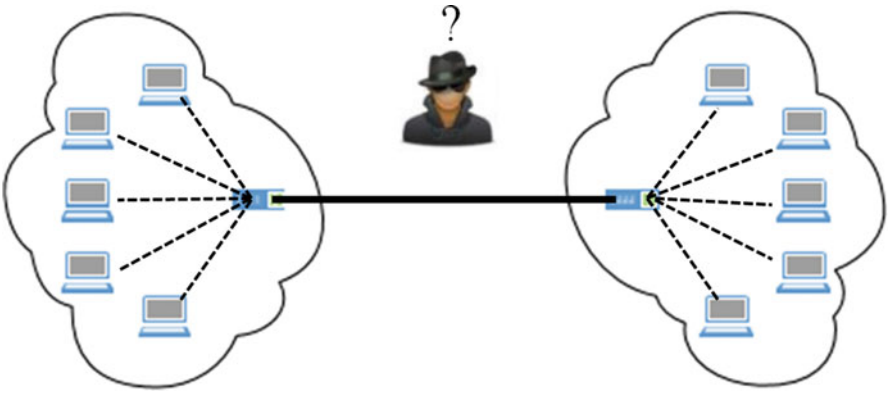


Fig. 6 Attacker's view of a communication between two hosts

while MT6D can prevent them by rotating the IP addresses. Hosts' privacy is also preserved by MT6D because of leveraging dynamic obscuration of the hosts' IP addresses. The dynamic obscuration prevents attackers to identify and track the hosts. It also prevents network traffic correlation because of changing the IP addresses multiple times during a single session.

In MT6D, dynamic interface identifier (IID) obscuration is leveraged to generate dynamic IP addresses. MT6D IIDs are computed through the use of three values:

- EUI-64 IID (Hinden and Deering 2006): The IEEE-defined 64-bit Extended Unique Identifier (EUI-64) is a static IID per each host across different subnets. It can be calculated based on the media access control (MAC) address of the host. Combination of these 64 bits with the subnet prefix (included in route advertisement messages of the subnet's router) performs a unique IPv6 unicast address for the host.
- Shared symmetric key: Two hosts should share a symmetric key before starting the MT6D. Out-of-band is suggested for sharing the key.
- Timestamp: Twice the single-trip time between the peer hosts is the minimum value of the time interval. After each time interval, the value of the current time is used as the timestamp in order to calculate the next IID.

Hash of these three values is calculated after each time interval. The leftmost 64 bits of this hash constructs a new IID. This new IID is used to generate a new IPv6 address per each host. After generating and registering the new IPv6 address, the previous one is removed by the host to prevent any connection attempt from attackers.

Putting the EUI-64 IID of the peer host in the same formula generates the IPv6 address of the peer host for the current time interval. In this way, each host can generate a new IPv6 address for itself and calculate the IPv6 address of its peer host.

Instead of rewriting original data packets, MT6D encapsulates them to Unreliable Datagram Protocol (UDP) packets and uses virtual IP addresses (dynamic IPv6

addresses) in their header. Architecture of single MT6D host includes an encapsulator and decapsulator.

MT6D encapsulator is responsible for transmitting outbound packets. When a new packet is ready to send to the peer host that supports MT6D, the encapsulator encrypts the packet and encapsulates it in a UDP packet and inserts the dynamic IP addresses in its header. Reverse process is done at the receiver by MT6D decapsulator.

Two suggestions are provided in Dunlop et al. (2011) for implementing MT6D. These suggestions are as follows:

- Embedded software: implementing MT6D as embedded software onto the host (host-based).
- Gateway device: implementing MT6D on a separate device (e.g., gateway). In this option, MT6D is transparent to the host useful to support hosts with different platforms. This implementation can be used as a gateway of a trusted environment to connect two private networks.

MT6D, however, has some drawbacks and limitations:

- Packet loss due to address conflict exists. Address conflict may occur because of selecting random IP addresses. Although, the probability of an address conflict is very small in the seemingly endless supply of IP addresses in IPv6, it can disrupt the connection during the whole rotation interval that an address conflict occurs.
- Key management is lacking. Rekeying is needed in order to limit the amount of encrypted data with the same shared key. Typically a separate key exchange protocol is needed to prevent key recovery attacks. However, the MT6D method lacks support for key exchange protocols.
- Relatively tight time synchronization is needed. Lack of an accurate time synchronization method may cause incorrect prediction of the peer's current IP address.
- Dynamic address rotation interval is not supported. If a suspicious activity is detected by a host (e.g., being under attack), there is no way for the host to change its IP address before the end of the current time interval. Therefore, a dynamic address rotation interval is desirable depends on the network situations.

MTM6D

Moving target mobile IPv6 defense (MTM6D) (Heydari and Yoo 2016) is designed to improve the security of a server that is connected to a predefined number of clients. The main goal of the MTM6D method is preventing remote address-based attacks against the server through the use of IP hopping. By using a network layer moving target defense, a secure connectivity is maintained with authorized clients. Meanwhile, the server cannot be located for exploitation.

Though the server is not actually mobile, the server is treated as if it were a mobile node with implemented Mobile IPv6 protocol. According to the standard of Mobile IPv6, an MN has two types of addresses, HoA and CoA, as explained in section "Mobile IPv6." The HoA of the MN is used as a permanent IPv6 address of the server to be transparent to upper layers (to avoid disrupting TCP sessions). The CoA is used to connect to the clients.

Mobile IPv6 is selected as the base of MTM6D because of these reasons:

- Large address space of IPv6 is leveraged to ensure sufficient entropy in the address randomization.
- Because of disconnecting the HA from the network, the HoA of the server (permanent IP address) is not accessible through the Internet. The server's CoA is the only accessible IP address of the server that is rotated randomly and dynamically.
- Because of using Mobile IPv6 implementation, clients are able to cache the binding of the HoA of the server with its CoA. In this way, the clients can directly send packets to the server through the use of the server's CoA.
- Because of using the binding update mechanism of Mobile IPv6, authorized clients are updated with the new CoA of the server.

After each rotation interval, a new random IP address is generated by the server. After successful registration of this new IP address on the router (avoid any address conflict), the server removes its previous CoA. In this case, the Mobile IPv6 implementation of the server will automatically send BU messages to update all clients with the new CoA of the server. Therefore, MTM6D does not have any packet loss due to address conflict.

If the server detects any attack from one of its clients, the server can stop sending BU messages to this malicious client. Therefore, the malicious client will not have access to the server after one rotation interval.

Probability of packet loss during address rotations and the extra overhead caused by sending BU (and BA) messages are two drawbacks of the MTM6D method. The overhead comparison between MTM6D and MT6D is shown in Fig. 7. In this comparison, a connection between two hosts is considered. According to the paper, if the mean number of packets per second is greater than one, the overhead per packet of MTM6D will be less than MT6D.

MVPN

A hybrid scheme (MVPN) of utilizing the MTM6D method along with an intrusion detection scheme is presented in Heydari et al. (2016b). This scheme is designed for building secure VPNs with MTM6D. MVP uses a dynamically adjustable shuffle time on the server based on the level of trust over the clines. A long shuffling interval is used by default, and if an attack is detected, the IP address of the server is shuffled. Furthermore, a new method is presented to detect and isolate internal attacker. The

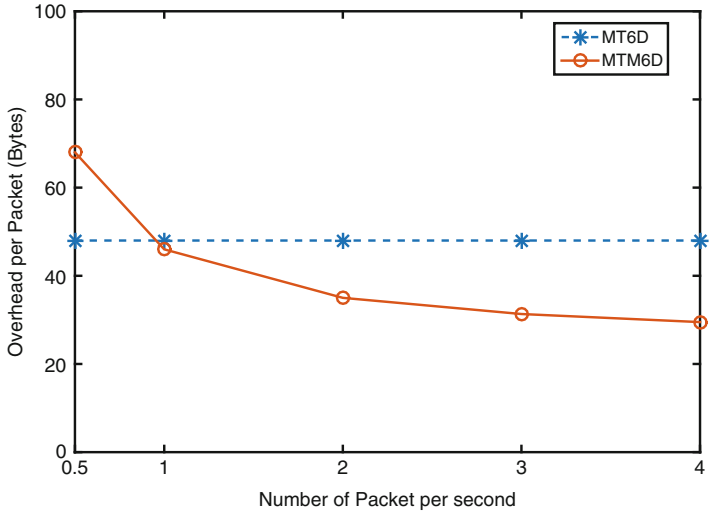


Fig. 7 Overhead per packet as a function of number of packets per second

issue of internal attack isolation was discussed in MTM6D (Heydari and Yoo 2016). Keeping these attackers' IP addresses in a blacklist and not updating them with the new CoA of the server was suggested in the MTM6D method. However, coordination between two attackers (collusion attack) was not considered in MTM6D. For example, one of attackers can act like a normal client and receive the BU messages and share the new CoA of the server with another attacker who actually attacks to the server. This attack is illustrated in Fig. 8. In this case, the real attacker cannot be detected by the server because the attacker's IP address is not registered as a client of the server.

MVPN proposed a solution to detect any internal attackers or a client who share the CoA of the server with an external attacker. In order for this strategy to work, the MVPN method uses multiple CoAs distributed to different clients. At its simplest form, an IP address (CoA) can be assigned for each client. In this way, each client is responsible for its assigned IP address of the server. If any attacks are detected by the IDS on the server, the covert client who is sharing the BU messages of the server with an attacker can be detected, because only this client knows the IP address of the server that is under attack.

Design

To enable a more effective MTD, MVPN leverages multiple CoAs bound to a single server. The server is treated as if it were an MN. Note that actual mobility is not needed in the server. The HoA of the MN (server) is used as the server's permanent IP address. Different CoAs of the server are used for communicating with different clients.

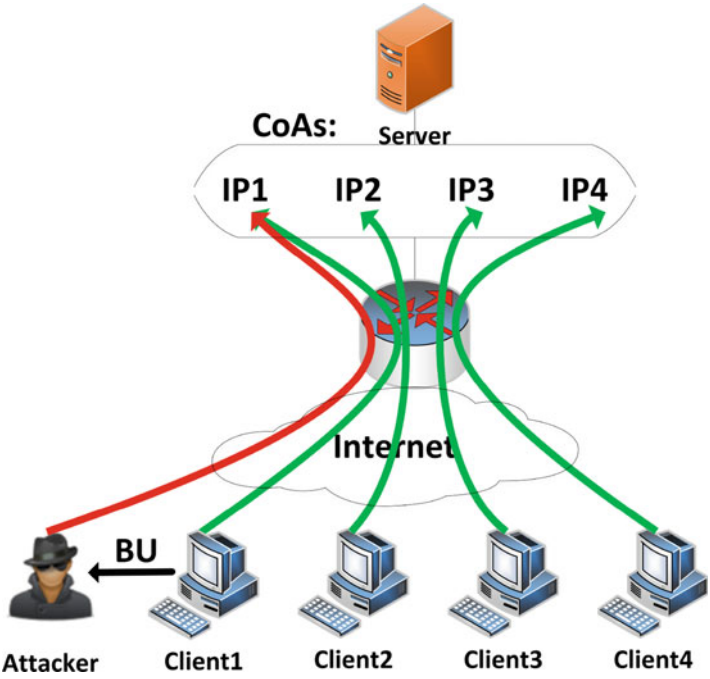


Fig. 8 Collusion attack

Pseudo-random IP selection is leveraged to generate these CoAs after each time interval (*shuffling interval*). During each shuffling interval, a new CoA is generated per each client. The clients are notified through the use of BU messages. Note that the real HA is not utilized in this method. More specifically, Mobile IPv6 is implemented on the server and an IP address with a prefix different from the server's subnet is assigned as the HoA of the server. In this case, the prefix of the home link in route advertisement messages from the subnet's router will look different from the prefix of the HoA. Therefore, according to Mobile IPv6, the server assumes that it is in a foreign network and registers a CoA.

The server combines the advertised prefix with a randomly generated 64-bit IPv6 addresses to create new CoAs. These new CoAs are checked against current occupancy by sending neighbor solicitation messages. If address conflicts are not detected, the CoAs are registered on the subnet. Then, the Mobile IPv6 implementation on the server will notify the clients of the new CoAs via BU messages. After this process, previous CoAs of the server are discarded. Receiving BU messages helps each client to update its binding cache with the server's HoA and the received CoA.

Note that according to the return routability procedure (explained in section "Return Routability Procedure"), the HA is needed for route optimization. However, in the scheme explained in RFC 4449 (Perkins 2006), all messages related to the

return routability procedure are eliminated through the use of a shared symmetric key. This approach is leveraged in MVPN to decrease the signaling overhead for route optimization and minimize the handoff delay accordingly. Furthermore, the HA is no longer used for route optimization. Therefore, the static IPv6 address of the server (HoA) is not accessible through the Internet and VPN is not vulnerable to address-based attacks. However, new clients also cannot start contacting the server. In fact, only the server can initiate a connection. Therefore, new clients should use an out-of-band method to ask the server for communication.

Different solutions can be used for the out-of-band registration. For example, authenticated email messages can be implemented for a corporate VPN. Each authenticated email message should include the client's IPv6 address and a way for authentication. For example, a secret key or password of the client encrypted by the server's public key may be used. When the server receives and verifies the credentials, a unique ID for the client is generated. Upon successful verification, connection can be started by the server via sending out a ping message to the client. The standard implementation of Mobile IPv6 automatically starts the route optimization mechanism to notify the client with an active CoA that is assigned to this client.

The server keeps a list of the clients. Each entry of this list includes a client's IPv6 addresses, ID, and mode information. The mode information includes three different modes, (*normal*, *suspicious*, or *malicious*). The normal mode is used by default for each new client. Each mode has a different shuffling interval. The shuffling interval of the normal mode (t_n) is longer than the shuffling interval of the suspicious mode(t_s).

Attack Handling

An IDS is utilized on the server to detect potential attacks. If any suspicious activity is detected, the server can identify the client that was associated to the CoA under attack. This client may be innocent because the attacker may have used an IP scan. Therefore, the client should not be placed in the malicious mode immediately. In fact, the client should be placed in suspicious mode that has a shorter shuffling interval. If another attack is detected to the CoA assigned to this client, the client is placed in the malicious mode. This mode is like a blacklist for the VPN and clients placed in this mode will not be updated with new CoAs of the server. This process is shown in Fig. 9.

Note that the malicious client may change its IP address and attempt to reregister as a new client. However, this way does not help the malicious client because of the credential verification process on the server. If the credential of a new client matches a client in malicious mode, the server does not accept it. More preciously, when a new connection is established for a client, the same mode of this client during previous session will be used. Hence, changing the IP address does not change the mode of the malicious client.

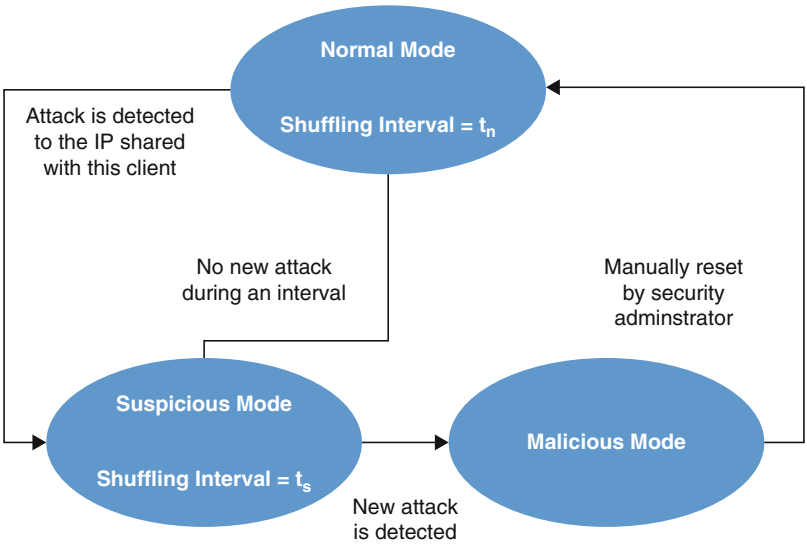


Fig. 9 Different operating modes

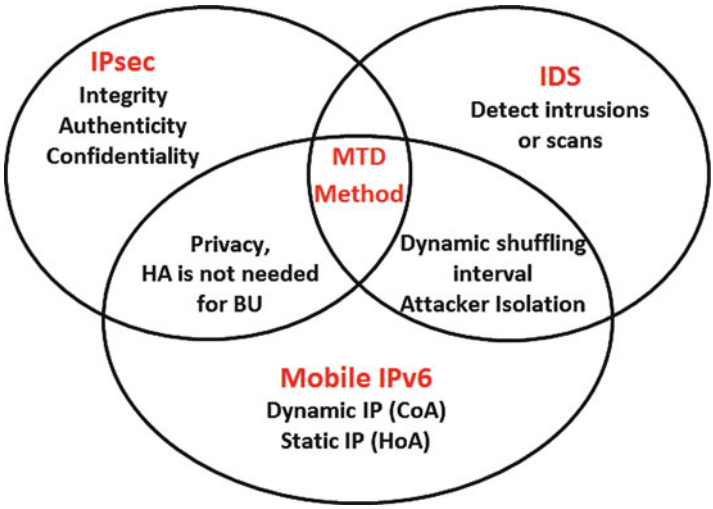


Fig. 10 Design concept of MVPN approach

The design concept of MVPN is illustrated in Fig. 10. MVPN uses combination of standard protocols instead of creating a new protocol because a new protocol can add new vulnerabilities to the server and may have scalability or security problems. More specifically, MVPN uses a combination of Mobile IPv6, IPsec, and IDS.

Scalability

Two scalability issues of the MVPN method is explained in Heydari et al. (2016b). The number of IPv6 addresses needed by the server is one these scalability issues. Another one is finding a way to update the shared keys used for the route optimization procedure.

According to the experimental results of Morrell et al. (2014), it is possible to bind 55,000 IPv6 addresses to a single computer in the amount of time that is necessary for normal network operation. The worst case for MVPN is having all clients in suspicious mode. In this case, the shortest shuffling interval is used (e.g., $t_s = 10$ s). According to the results of Morrell et al. (2014), the server can be able to bind 10,000 IPv6 addresses every 10 s. It is important to note that this number of bound IPv6 addresses may be increased depending on the number of network interfaces or servers used in the VPN. For the second scalability issue, the use of IPsec with Internet Key Exchange ver. 2 (IKEv2) (Kaufman et al. 2014) is proposed for MVPN. MVPN uses IPsec with IKEv2 for encryption, authentication, key distribution/rekeying, and replay attacks protection. Therefore, MVPN does not depend on a specific algorithm or key size for encryption, authentication, and key distribution. This portability feature helps MVPN to be implemented for different applications. For example, assume that the clients are small low-power Internet of Things (IoT) devices. In this case, the choice of cryptographic algorithms is left to negotiation steps of IKEv2 for selecting an algorithm that both server and IoT devices support.

Implementation Results

A proof-of-concept prototype of the MVPN scheme is explained in Heydari et al. (2016b) to evaluate its performance. The ipv6 test bed is shown in Fig. 11. In this test bed, four routers and eight computers running Ubuntu Linux version 14.04 are used. To implement Mobile IPv6, the mobility is enabled on the kernel of Ubuntu and the kernel is recompiled and UMIP, an open source implementation of Mobile IPv6, is used. In this test bed, the core of the Internet is emulated by router R1.

The prefix of the server's HoA is not the same as the advertised prefix via R2. Therefore, a unique CoA per each client is registered by the server. Subsequently, BU messages are sent to update each client with one of these CoAs.

A shuffling management function is added to the source code of UMIP. This function is responsible for periodically checking a client list on the server. The shuffling interval of the normal mode (t_n) is set to 1 min. During each shuffling interval, the server generates seven random CoAs and removes the previous CoAs. Then, the Mobile IPv6 implementation on the server automatically updates the clients through the use of BU messages.

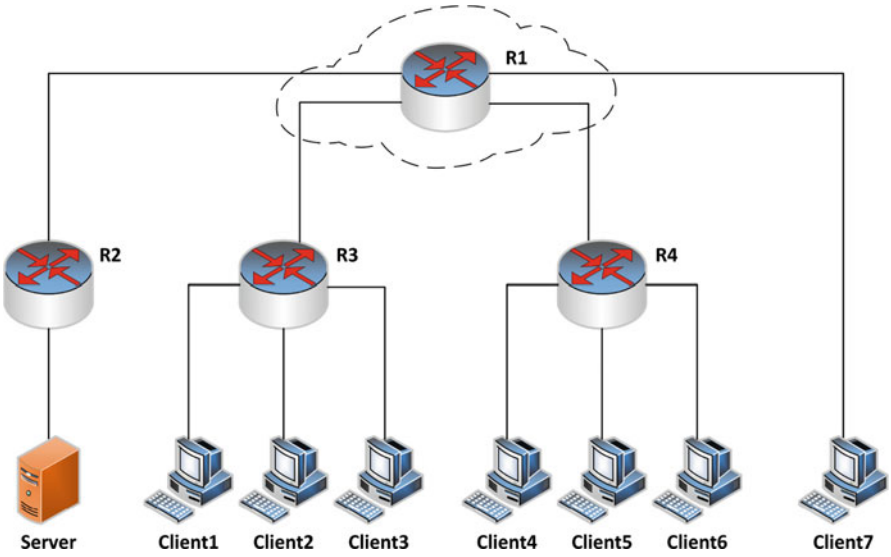


Fig. 11 The network topology of the test bed

Either (or both) signature-based or anomaly-based IDS can be used as a plugin-like module. For the test, signature-based network intrusion detection system (Snort (*Scapy* n.d.)) is used. Snort is one of the tools that can easily be added into the MVPN implementation. If snort detects an attack, the attacked IP address of the server will be written to a file. This file is checked by the new function added to UMIP. The function can find the client that knows this attacked IP address of the server. Then, the client's mode will be downgraded accordingly from the normal mode to the suspicious mode or from the suspicious mode to the malicious mode. Note that this downgrading can be done automatically because of the low false positive rates of the Snort (or other signature-based intrusion detection methods).

Anomaly-based IDS can also be used if zero-day vulnerabilities are important for the network operator. Since anomaly-based intrusion detection methods normally have higher false positive compared with signature-based, some manual inspection steps can be done before downgrading a client. It is one of the best advantages of MVPN that is designed based on a combination of three independent standard protocols. In fact, changing one of them does not affect the others.

For testing purposes, to observe the different shuffling intervals, clients' mods are edited manually to simulate an attack while the server was online. The impact of such an attack on the shuffling interval is illustrated in Fig. 12. Each shuffling interval is represented by a vertical line. About 10 s is assumed for the shuffling interval of the suspicious mode. The client that is in the suspicious mode can be upgraded back to the normal mode if it is not detected again as an attacker.

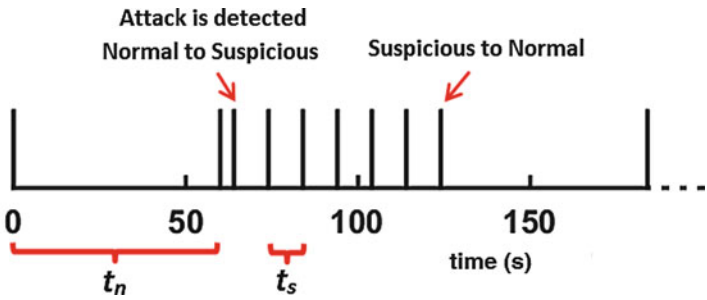


Fig. 12 Effect of attack on shuffling interval

Overhead and Optimization

MVPN adds two different types of overheads. One of them is signaling overhead. Signaling overhead is created by some extra packets used for updating clients with new CoAs (BU and BA messages). Note that BA messages are used as confirmations of received BU messages. When the server sets the ACK bit in BU message, the client who receives this BU message should send back a BA message. Using BA messages helps the server to ensure that its clients have received and updated their binding cache entries. After each shuffling interval, two signaling packets are generated (one BU and one BA) per each client. The update procedure is illustrated in Fig. 13.

An optimization is suggested in Heydari et al. (2016b) to reduce the signaling overhead. It was suggested to operate MVPN without using BA messages during a safe operating condition. After sending BU messages, a data packet from a client to a new CoA (assigned to this client) of the server can be used as a confirmation of receiving the BU message. In order for this strategy to work, the server may need to keep open more than one CoA per each client. Note that the server can request for explicit BA messages from its clients if an intrusion is detected. A BU message of the standard Mobile IPv6 protocol has a flag to specify whether a BA message is requested for this BU message or not. Therefore, modifications on the standard Mobile IPv6 are not needed for utilizing this suggested optimization.

The second type of overhead made by MVPN is transmission overhead. Each data packet transmitted by the server should have the type 2 routing header (24 extra bytes) to store the HoA of the server. There is also the destination option header for the same purpose for data packets transmitted by clients. Furthermore, another 24 bytes of overhead exists because of using IPsec with ESP protocol. Actually, the extra 24 bytes due to the use of IPsec is not caused by the MVPN method and is very common overhead for any secure communication utilizing IPsec ESP.

Counting the 24 bytes of IPsec, each signaling message (BU or BA) is 134 bytes. Note, however, that the size of each BU and BA message in the standard Mobile

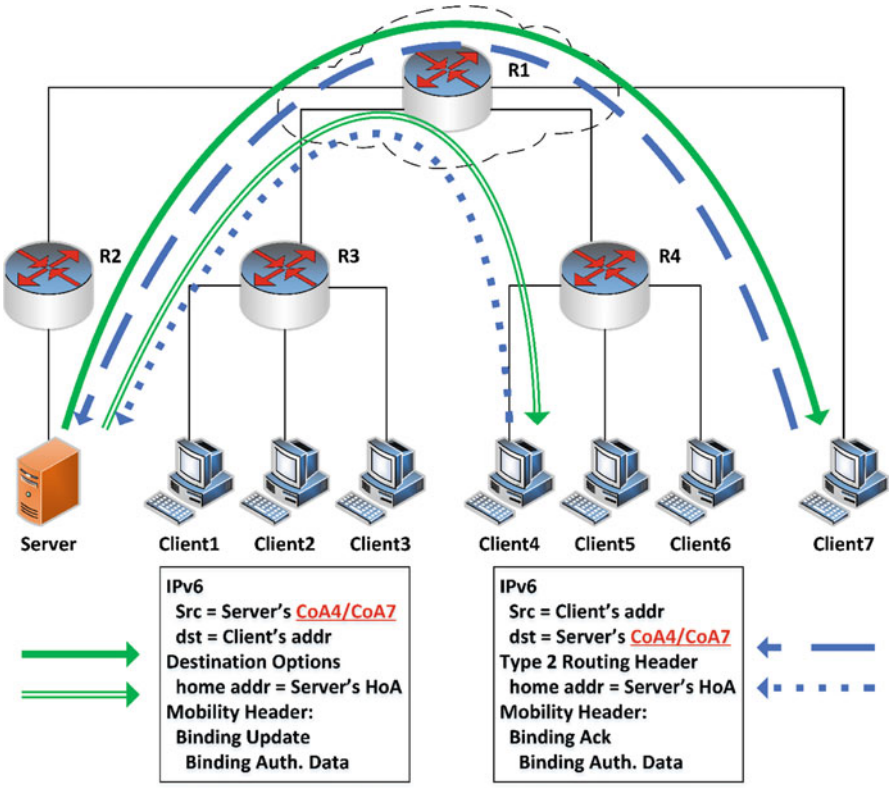


Fig. 13 The binding update process

IPv6 is 110 bytes, but there are also some extra packets (four packets) due to the use of the return routability procedure. Therefore, the final overhead of route optimization in the standard Mobile IPv6 is 660 bytes (that is, 268 bytes in MVPN).

Handoff Delay

After each shuffling interval, when the server registers new CoAs and removes previous CoAs, a handoff delay occurs that can result in some packet loss. During the handoff delay, all packets on the way have the old CoAs (now defunct CoAs) on their headers. Therefore, these packets will not be delivered. This issue is illustrated in Fig. 14. Depending on using User Datagram Protocol (UDP) or Transmission Control Protocol (TCP), these lost packets will be ignored or retransmitted, respectively. As can be seen in Fig. 14, this handoff delay equals the round trip time between the server and the client.

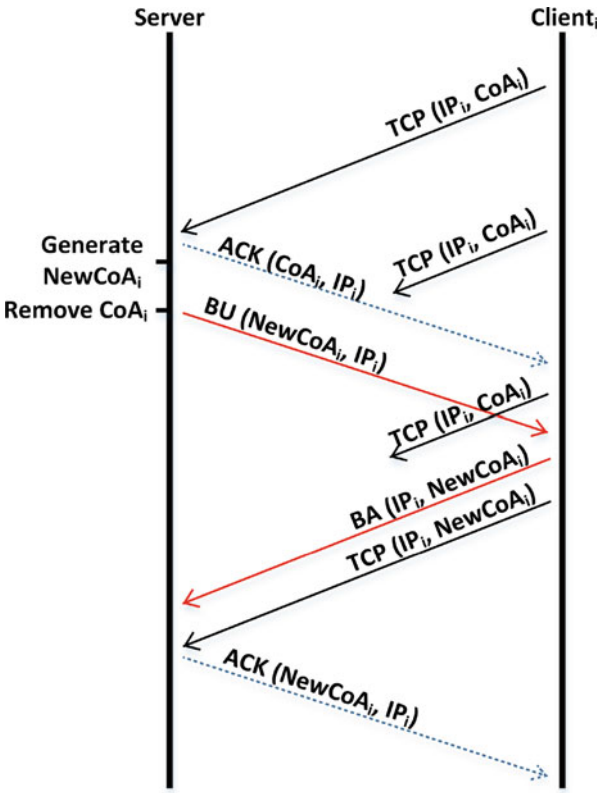


Fig. 14 Dropping packets during the handoff delay

UDP Test

For this test, one of the clients sends UDP packets to the server. About 200 ms is the round trip time between the client and the server. Therefore, the handoff delay equals 200 ms. The handoff delay ratio depends on the size of shuffling interval. Using 10 s for the shuffling interval (the default value for the suspicious mode), the handoff delay ratio equals $(0.200/10) = 2\%$. Note that the packets were generated by each client from 100 ms before the issuing of BU messages to 100 ms after that will be lost. For the normal mode, the default shuffling interval equals to 60 s. Therefore, the handoff delay ratio equals $(0.200/60) \approx 0.33\%$. The experimental results based on different packet generation rates are shown in Table 1. D-ITG (*D-ITG, Distributed Internet Traffic Generator* n.d.) is used to generate UDP packets.

TCP Test

Another test is done based on sending TCP packets from a client to the server. According to the standard TCP protocol, when a transmitter does not receive an

Table 1 Packet loss rates (UDP test)

	Packet loss rate	
Number of packets per second	10s	60s (%)
10	1.80%	0.33
100	1.82%	0.31
1000	1.79%	0.30

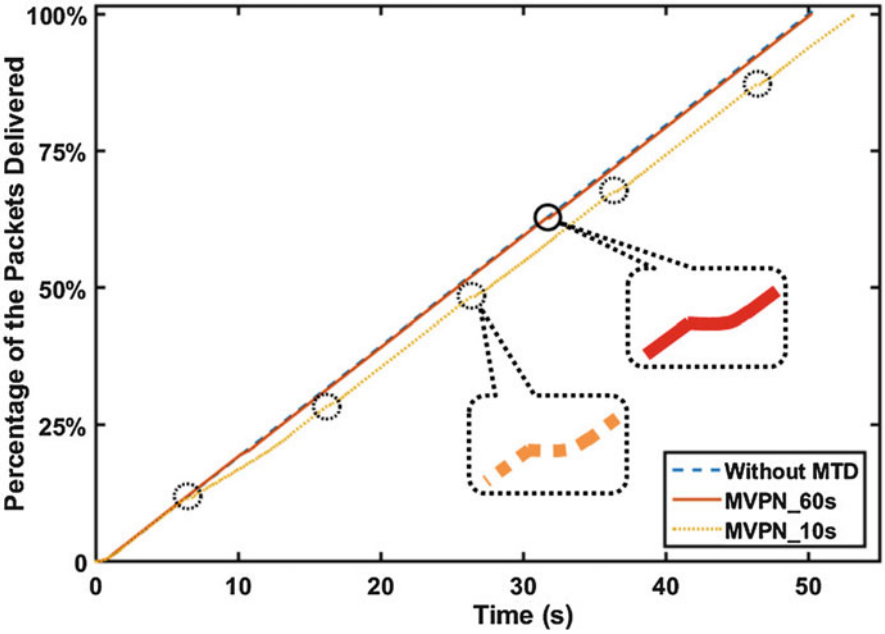


Fig. 15 Percentage of TCP packets delivered over time

ACK packet for a sent packet, the transmitter should send the packet again. In this test, the client sent 1000 TCP packets during 50 s. The size of each TCP packet was 500 bytes.

Slow start and congestion avoidance (Allman et al. 2009) algorithms were used by a TCP transmitter to achieve congestion avoidance caused by injecting more data than the network's maximum carrying capacity. When a new TCP transmission is started, TCP slowly tests (slow start) the network capacity to avoid congesting with inappropriately high speed transmission. The slow start is also used after repairing a lost connection. More specifically, when TCP does not receive the ACK packets, TCP experiences timeout and resends the unacknowledged packets and reduced the transmission speed. The slow start is shown in Fig. 15 with circles. This figure shows the handoff delay for 10 s and 60 s shuffling interval.

Conclusion

Preventing remote attacks in reconnaissance step, the first step of intrusion kill chain, is highly recommended to reduce the cost and damage caused by any attack. An effective defense is a mechanism to change the IP addresses randomly and dynamically (IP hopping). In this chapter, some novel moving target defense methods based on IPv6 (MT6D) and Mobile IPv6 (MTM6D and MVP) were explained to thwart remote attacks by randomly changing the IP address(es) of the target(s).

These MTD solutions may also be combined with existing defensive methods to form a robust defense-in-depth solution.

The Mobile IPv6-based moving target defense strategy (MTM6D and MVPN) can also be used on the side of information purveyors for combating censorship. For this goal, the MTD method can be leveraged to make it impractical and too expensive for adversaries to censor web sites (Heydari et al. 2016a, 2017).

Compared with MTM6D and MVPN, The best advantage of MT6D approach lies in the fact that this approach maintains user privacy as well. On the other hand, MVPN (improved version of MTM6D) has significant improvements in terms of availability, flexibility, independence, etc.

Although the first step has taken to improve MT6D for client server network support (Morrell et al. 2014), MT6D was focused solely on peer-to-peer networks in its original design and implementation. Therefore, the scalability issue of MT6D (and MVPN) remains to be investigated.

References

Allman, M., Paxson, V., & Blanton, E. (2009, September). *TCP congestion control* (No. 5681). RFC 5681 (Draft standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc5681.txt

Conta, A., Deering, S., & Gupta, M. (2006, March). *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification* (No. 4443). RFC 4443 (Draft standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc4443.txt (Updated by RFC 4884).

Danev, B., Masti, R. J., Karame, G. O., & Capkun, S. (2011). Enabling secure VM-vTPM migration in private clouds. In *Proceedings of the 27th annual computer security applications conference* (pp. 187–196). New York: ACM. https://doi.org/10.1145/2076732.2076759.

Deering, S., & Hinden, R. (1998, December). *Internet Protocol, Version 6 (IPv6) Specification* (No. 2460). RFC 2460 (Draft standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc2460.txt (Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946, 7045, 7112).

D-ITG, Distributed Internet Traffic Generator. (n.d.). http://traffic.comics.unina.it/software/ITG/. Accessed 24 Mar 2016.

Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., & Carney, M. (2003, July). *Dynamic host configuration protocol for IPv6 (DHCPv6)* (No. 3315). RFC 3315 (Proposed standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc3315.txt (Updated by RFCs 4361, 5494, 6221, 6422, 6644, 7083, 7227, 7283, 7550).

Dunlop, M., Groat, S., Urbanski, W., Marchany, R., & Tront, J. (2011). Mt6d: A moving target ipv6 defense. *Afcea/IEEE Milcom*.

Gil, T. M., & Poletto, M. (2001). MULTOPS: A data-structure for bandwidth attack detection. In *Proceedings of the 10th conference on usenix security symposium volume 10*. Berkeley: USENIX Association.

Gude, N., Koponen, T., Pettit, J., Pfaff, B., Casado, M., McKeown, N., & Shenker, S. (2008, July). NOX: Towards an operating system for networks. *SIGCOMM Computer Communications Review, 38*(3), 105–110. https://doi.org/10.1145/1384609.1384625.

Heydari, V., & Yoo, S.-M. (2016). Securing critical infrastructure by moving target defense. In *11th international conference on cyber warfare and security (ICCWS 2016)*, Boston, MA.

Heydari, V., Kim, S.-I., & Yoo, S.-M. (2016a). Anti-censorship framework using mobile ipv6 based moving target defense. In *ACM cyber and information security research conference*, Oak Ridge, TN.

Heydari, V., Yoo, S.-M., & Kim, S.-I. (2016b, Dec). Secure VPN using mobile ipv6 based moving target defense. In 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC

Heydari, V., Kim, S.-I., & Yoo, S. M. (2017). Scalable anti-censorship framework using moving target defense for web servers. *IEEE Transactions on Information Forensics and Security.* https://doi.org/10.1109/TIFS.2016.2647218.

Hinden, R., & Deering, S. (2006, February). *IP Version 6 addressing architecture* (No. 4291). RFC 4291 (Draft standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc4291.txt (Updated by RFCs 5952, 6052, 7136, 7346, 7371).

Hong, J. B., & Kim, D. S. (2016, March). Assessing the effectiveness of moving target defenses using security models. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 163–177. https://doi.org/10.1109/TDSC.2015.2443790.

Hussain, A., Heidemann, J., & Papadopoulos, C. (2003). A framework for classifying denial of service attacks. In *Proceedings of the 2003 conference on applications, technologies, architectures, and protocols for computer communications* (pp. 99–110). New York: ACM. https://doi.org/10.1145/863955.863968.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In *6th annual international conference on information warfare and security*, Washington DC.

Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2012). OpenFlow random host mutation: Transparent moving target defense using software defined networking. In *Proceedings of the first workshop on hot topics in software defined networks* (pp. 127–132). New York: ACM. https://doi.org/10.1145/2342441.2342467.

Jankiewicz, E., Loughney, J., & Narten, T. (2011, December). *IPv6 node requirements* (No. 6434). RFC 6434 (Informational). IETF. Retrieved from http://www.ietf.org/rfc/rfc6434.txt

Jia, Q., Wang, H., Fleck, D., Li, F., Stavrou, A., & Powell, W. (2014). Catch me if you can: A cloud-enabled DDoS defense. In 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Atlanta, GA, pp. 264–275.

Johnson, D., Perkins, C., & Arkko, J. (2004, June). *Mobility support in IPv6* (No. 3775). RFC 3775 (Proposed standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc3775.txt (Obsoleted by RFC 6275).

Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (2014, October). *Internet key exchange protocol version 2 (IKEv2)* (No. 7296). RFC 7296 (Internet standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc7296.txt (Updated by RFCs 7427, 7670).

Kent, S. (2005a, December). *IP authentication header* (No. 4302). RFC 4302 (Proposed standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc4302.txt

Kent, S. (2005b, December). *IP Encapsulating Security Payload (ESP)* (No. 4303). RFC 4303 (Proposed standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc4303.txt

Kent, S., & Seo, K. (2005, December). *Security architecture for the internet protocol* (No. 4301). RFC 4301 (Proposed standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc4301.txt (Updated by RFCs 6040, 7619).

Manadhata, P. K., & Wing, J. M. (2011). An attack surface metric. *IEEE Transactions on Software Engineering, 37*(3), 371–386. https://doi.org/10.1109/tse.2010.60.

Morrell, C., Ransbottom, J. S., Marchany, R., & Tront, J. G. (2014, Dec). Scaling ipv6 address bindings in support of a moving target defense. In *The 9th international conference for internet technology and secured transactions (icitst-2014)* (p. 440–445). https://doi.org/10.1109/ICITST.2014.7038852.

Narten, T., Nordmark, E., Simpson, W., & Soliman, H. (2007, September). *Neighbor discovery for IP version 6 (IPv6)* (No. 4861). RFC 4861 (Draft standard), IETF. Retrieved from http://www.ietf.org/rfc/rfc4861.txt (Updated by RFCs 5942, 6980, 7048, 7527, 7559, 8028).

Okhravi, H., Comella, A., Robinson, E., & Haines, J. (2012). Creating a cyber moving target for critical infrastructure applications using platform diversity. *International Journal of Critical Infrastructure Protection, 5*(1), 30–39. https://doi.org/10.1016/j.ijcip.2012.01.002.

Perkins, C. (2006, June). *Securing mobile IPv6 route optimization using a static shared key* (No. 4449). RFC 4449 (Proposed standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc4449.txt

Perkins, C. (2010, November). *IP mobility support for IPv4, Revised* (No. 5944). RFC 5944 (Proposed standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc5944.txt

Perkins, C., Johnson, D., & Arkko, J. (2011, July). *Mobility support in IPv6* (No. 6275). RFC 6275 (Proposed standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc6275.txt

Scapy. (n.d.). http://www.secdev.org/projects/scapy/. Accessed 24 Mar 2016.

Stavrou, A., Keromytis, A. D., Nieh, J., Misra, V., & Rubenstein, D. (2005, February). Move: An end-to-end solution to network denial of service. In *Proceedings of the internet society (ISOC) symposium on network and distributed systems security (SNDSS)*. San Diego.

Thomson, S., Narten, T., & Jinmei, T. (2007, September). *IPv6 stateless address autoconfiguration* (No. 4862). RFC 4862 (Draft standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc4862.txt (Updated by RFC 7527).

Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., & Nagami, K. (2009, October). *Multiple care-of addresses registration* (No. 5648). RFC 5648 (Proposed standard). IETF. Retrieved from http://www.ietf.org/rfc/rfc5648.txt (Updated by RFC 6089).

Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., & Stavrou, A. (2014). A moving target DDoS defense mechanism. *Computer Communications, 46*, 10–21. https://doi.org/10.1016/j.comcom.2014.03.009.

Zhang, Y., Li, M., Bai, K., Yu, M., & Zang, W. (2012). Incentive compatible moving target defense against VM-colocation attacks in clouds. In D. Gritzalis, S. Furnell, & M. Theoharidou (Eds.), *Information security and privacy research: 27th ifip tc 11 information security and privacy conference, sec 2012, Heraklion, Crete, June 4–6, 2012. Proceedings* (pp. 388–399). Berlin/Heidelberg: Springer.

Assessing the Risk of Ports and Their Supply Chains: The CYSM, MEDUSA, and MITIGATE Approaches

47

Nineta Polemi and Spyridon Papastergiou

Contents

Introduction

In the modern era, the ports' Supply Chains (SCs) are the blood veins of global trade and subject to protection in political crisis and warfighting. Nowadays, these ports' SCs (e.g., container management, vehicle transport, liquefied natural gas (LNG) storage and transport, cruising) are very complex, diverse and involve many cross border partners (e.g., governmental bodies, maritime companies, airports, railways,

Associate Professor Nineta Polemi served as technical and project manager of the European projects CYSM, MEDUSA, and MITIGATE.

N. Polemi (✉) · S. Papastergiou
UNIPI Security Lab, Department of Informatics, University of Piraeus, UNIPI, Pireaus, Greece
e-mail: dpolemi@gmail.com; paps@unipi.gr

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_53

energy providers, banks, transport/logistic companies) operating within their SCs having physical and cyber multi-interdependencies, interacting with all sectors of economy. For example, most physical processes in ports (e.g., vehicles and cargo loading/unloading, LNG distribution and storage) are executed with autonomous or semiautonomous systems under the control of sophisticated logistic software systems (e.g., Industrial Cyber-Physical Systems, SCADA). These cyber-physical systems are connected around the world through cyberspace with other SC operators (e.g., ship industry, trading, transport, maritime, and logistics companies) to ensure a seamless and swift data exchange and with that swift and seamless trade from the producer down to the end consumer.

However, the main issue is that malicious activities in the cyber-physical systems might constrain the free flow of trade disturbing or even disrupting the operation of the port-related SCs. In particular, these operations have become lately subject of various cyber, physical and combined attacks on their physical and cyber systems causing tremendous damage to the maritime operations, national and E.U. economies. Nowadays, a variety of criminals ranging from individuals and groups like anonymous acting for ideological or political reasons, over cyber criminals, to terrorists and states exists. Their motivations vary on political or military advantage when it comes to state actors, financial gain when it comes to cyber criminals, and ideological and religious advantage when it comes to terrorists. For example, attacks in the Industrial Control Systems (ICSs) (e.g., supervisory control, SCADA, distributed control systems, and programmable logic controllers) hosted in ports or maritime transport companies may cause disruption or damage of critical mechanical devices (e.g., container cranes, safety and mechanical systems that operate locks and dams) and even worse they may cause loss of life, steal of cargo, destroy of ship, and final disruption of the SCs. Just imagine the effects (in terms of thermal radiation, overpressure blast wave, and flying shrapnel) of the explosion of a liquefied-natural-gas tanker in the port of Hamburg that explodes due to a hacked SCADA system. In addition, a security incident in the ports' LNG storage facilities or in the SC terminals could have detrimental consequences to the well-being, health, and safety of citizens, along with economic consequences, and impact on the productivity and development of societies and countries; for example, it could lead to lack of energy stock, which could be critical during cold waves, affecting not only the economy but more importantly the citizenship wellness and health integrity.

Several recent studies have shown that the cyber threats landscape is changing continuously and the nature of attacks of this sort are evolving and are becoming even more targeted, sophisticate, and ingenious; thus, the cyber criminals will continue to do the unexpected discovering new ways to break into ICT maritime supply chain. In particular, in the last 3 years, the ports' SCs have garnered front-page attention as victims of cyber-attacks: (i) A Chinese manufacturer implanted malware in inventory scanners to steal supply chain intelligence; (ii) Hackers recently shut down a floating oil rig by tilting it; (iii) Somalian pirates used low-cost GPS jammers to change a vessel's course by interfering with its navigation systems (GPS, ECDIS, and AIS), causing a trackline-following autopilot to

inaccurately interpret the ship's position and alter its course; (iv) Hackers gained access to shipping company's databases and vessel tracking systems to identify vessels with valuable cargo, thus many ships that transit the Gulf region are turning their AIS navigation tracking system off so that pirates cannot identify, locate, and track them; (v) In port of Antwerp, between 2011 and 2013, cyber-attacks were used to highjack, divert, or steal cargo; (vi) Major maritime company engaged in a deal to order a seafloor mining vessel was the victim of a cyber-attack as it unknowingly pre-paid ($10 million of the $18 million charterer's guarantee) the deposit into a bank account that belonged to a cyber-criminal.

In this vein, enhanced, global risk assessment frameworks that can deal with ports ICT risks, cascading effects of ports risks to their supply chain, threats and vulnerabilities, of ICT-based maritime supply chain are needed (Polemi and Papastergiou 2015). This chapter presents the escalating results from three related projects: CYSM (http://www.cysm.eu/index.php/en/), MEDUSA (medusa.cs.unipi.gr), and MITIGATE (www.mitigateproject.eu) and concludes with various open issues for further research.

Risk Assessment Approaches

The main goal of risk management is (in general) to protect business assets and minimize costs in case of failures, and thus, it represents a core duty of successful company management. Hence, risk management describes a key tool for the security within organizations, and it is essentially based on the experience and knowledge of best practice methods. These methods consist of an estimation of the risk situation based on the business process models and the infrastructure within the organization. In this context, these models support the identification of potential risks and the development of appropriate protective measures. The major focus lies on companies and the identification, analysis, and evaluation of threats to the respective corporate values.

The outcome of a risk analysis is in most cases a list of risks or threats to a system, together with the corresponding probabilities. International standards in the field of risk management are used to support the identification of these risks or threats as well as to assess their respective probabilities. These standards range from general considerations and guidelines for risk management processes (e.g., International Standardization Organization 2009a, b; Austrian Standards Institute 2004) to specific guidelines for the IT sector (e.g., International Standardization Organization 2005, 2011, 2013; Bundesamt für Sicherheit in der Informationstechnik 2013; The Stationery Office (TSO) and Continual Service Improvement 2007; Common Criteria Working Group 2007) all the way to highly specific frameworks as, for example, in the maritime sector (e.g., European Commission 2004; International Standardization Organization 2007; International Maritime Organisation 2004). Most of these standards specify framework conditions for the risk management process but rarely go into detail on specific methods for the risk analysis or risk

assessment. This is one reason why often differences in the risk assessment arise within the specific areas of application, making a direct comparison of the results difficult.

In principle, choosing the right method and the right tool for risk analysis and risk evaluation proves to be complicated. In recent years, a number of concepts, algorithms, and tools have evolved from research, specially designed to protect the IT infrastructure and related systems. Since their historical background is settled in a business context, in these methods a quantitative risk assessment is usually performed based on monetary costs (see Peltier 2001; Schechter 2004) and the EBIOS method and the aforementioned ISO/IEC 27005:2013 standard (International Standardization Organization 2011). In this context, most of the methods and tools (see European Network and Information Security Agency (2010) for a comprehensive list) just use the commonly known rule of thumb "risk = probability × potential damage" (CCRA Working Group 2006). In practice, the selection of a specific risk-assessment tool is based on practical considerations and depends on how well the present terminology of the application can be mapped onto the predefined specific terminology of the risk assessment methodology.

In contrary to the aforementioned general and IT-specific guidelines for risk management, the security and risk management in the maritime sector a huge emphasis is laid on the physical and object security. In particular, the International Ship and Port Facility Security (ISPS) Code (International Maritime Organisation 2004) (as well as the respective EU regulation [EC725/2004]) defines a set of measures to enhance the security of port facilities and ships. Therein, methodologies to perform security assessments and to detect security threats are described and a guideline for the implementation of the respective security measures is given. Additionally, roles and responsibilities concerning maritime security at a national and international level are defined. Nevertheless, due to the increased interaction and exchange of information of ports with other critical infrastructures in the maritime ecosystem (e.g., port authorities, ministries, maritime companies, ship industry, etc.), the sole focus on physical security is not sufficient any more. Moreover, the security of the port's cyber-physical systems becomes equally important.

During the last 5 years, a number of initiatives and efforts attempting to deal with the risks and vulnerabilities of the port Critical Information Infrastructure (CII) ecosystem emerged, addressing its cyber and physical nature, the complexity and interdependencies of the CII assets involved. EU wide activities towards a holistic risk management framework for port and supply chain security have recently carried out in the CIPS program (cf. the projects CYSM and MEDUSA) and in the European program (H2020-DS-6-2014) for "Risk management and assurance models" (the MITIGATE project). These initiatives look in more detail into the security and risk management with regards to threats against the port's cyber-physical systems. In particular, they lay a special focus on the cascading effects in such a multisector environment as well as on the provision of support for security processes associated with the dynamic (ICT-based) international maritime supply chain. These three initiatives are described in details in the following sections.

Collaborative Cyber/Physical Security Management (CYSM) System

Introduction

The CYSM system (Fig. 1) is a Risk Assessment Toolkit (Papastergiou et al. 2015a; Papastergiou and Polemi 2014; Karantjias et al. 2014) which facilitates the ports' security team to efficiently identify, assess, and treat their security and safety incidents involving all port operators and users. The system adopts and implements a bouquet of flexible and configurable self-driven functions and procedures which constitute the conceptual pillars for building a solution that assists ports to improve their current cyber and physical level.

In this context, in order for the system to support sound decision-making, it:

- incorporates a conformance approach that checks and defines the compliance of the ports against the requirements, rules, and obligations imposed by a set of security management standards (ISO 27001, ISPS) and the relative security and safety legal and regulatory framework;
- incorporates a collaborative, multiattribute, group decision-making algorithm that collects the diverse security-related knowledge located in the ports and the results (e.g., threats, vulnerabilities metrics, prioritization of countermeasures) produced by the automated and semiautomated risk assessment routines and processes in order to: (i) determine the value of the information assets, (ii) identify the applicable threats and vulnerabilities that exist (or could exist), (iii) identify the existing controls and their effect on the risk identified, (iv) determine the potential consequences, and (v) prioritize the derived risks and ranks them against the risk evaluation criteria set in the context establishment;

Fig. 1 Collaborative cyber/physical security management system

- integrates a security policy growing mechanism that provides a flexible way for creating and updating customized security policies and procedures;
- implements a social, collaborative working environment, which will facilitate and encourage the ports to jointly work and cooperate, by exchanging ideas and information pertaining to security and safety issues and by allowing them to reach targeted solutions in a collaborative and time-effective manner.

The aforementioned elements are combined in an effective and efficient manner to develop the automated routines and workflows that comprise and construct the meaningful CYSM Security Assessment Services (Risk Analysis Services (RAS), Risk Management Services (RMS), and Document Management Services (DMS)). These services are fully customizable depending on the ports' security profile (like the enterprise size, the interdependencies with other IT systems, the services offered, the number of administrators, and the security and safety awareness level), covering various aspects such as complexity, automation, terminology, simplification, and understanding.

CYSM Components

From a conceptual perspective, the system integrates the following main components:

- *Community Portal*: This area is accessible by all users of the involved ports and comprises of:
  - Community collaboration suite: encapsulates a set of specialized Web2.0 elements (e.g., blogs, forums) suitable for e-collaborate, collecting and sharing knowledge. These elements enable ports to work together in building open working groups, providing diverse opinions, thoughts and contributions and sharing information, experience, and expertise.
  - Community e-Library: acts as the knowledge source of all ports' physical and cyber-related information (e.g., European legal and regulatory framework, security-related standards, specifications, methodologies, and frameworks).
- *Port Private Portal*: This area provides the appropriate functionality that enables the users to assess and improve the security and safety level of their port's infrastructure. Actually, this area executes the risk assessment processes and routines integrated in the system and consist of the following modules:
  - Port collaboration suite: encourages and facilitates members of each port to closely cooperate and exchange information and ideas during the risk assessments.
  - Port e-Library: is an inventory of confidential announcements, security and safety policies and procedures, guidelines, etc.
  - Administration module: allows customizing of the risk assessment's parameters (e.g., threats, vulnerabilities, controls).
  - Management module: allows the initiation of a risk assessment.
  - Risk Assessment module: gives the opportunity to the ports to identify and measure their threats, their vulnerabilities, and possible impacts.

– Security Policy Reporting module: facilitates the formulation of customized security and safety-related policies and procedures.
– Risk Assessment Results module: allows the review of the risk assessment results and the formulation of a mitigation plan.

These components are provided through customized intuitive and interactive Web Interfaces (including interactive screens, online forms, Dynamic Questionnaires) to represent the scenarios and steps as well as the information and content (e.g., requirements, rules, obligations, and recommendations of the standardization framework and regime) required by the supported risk self-assessment routines and functions, presented in the previous section.

CYSM System Architecture

The proposed CYSM Toolkit is an innovative, scalable Cyber/Physical Self-Assessment and Management System which facilitates the ports to efficiently identify, assess, and treat their security and safety issues. This toolkit incorporates and merges a set of integrated and interconnected modules.

The subsystems (depicted in Fig. 2) that comprise the CYSM Toolkit are the following:

- The Web Interactive component provides an intuitive, interactive, and graphical way (e.g., dynamic forms) to represent the information and content (e.g., requirements, rules, obligations, recommendations, and advices of the legal, regulatory, and standardization framework and regime as well as security and safety content required for automating technical control compliance, vulnerability checking, and security measurement activities) of the risk assessment services.

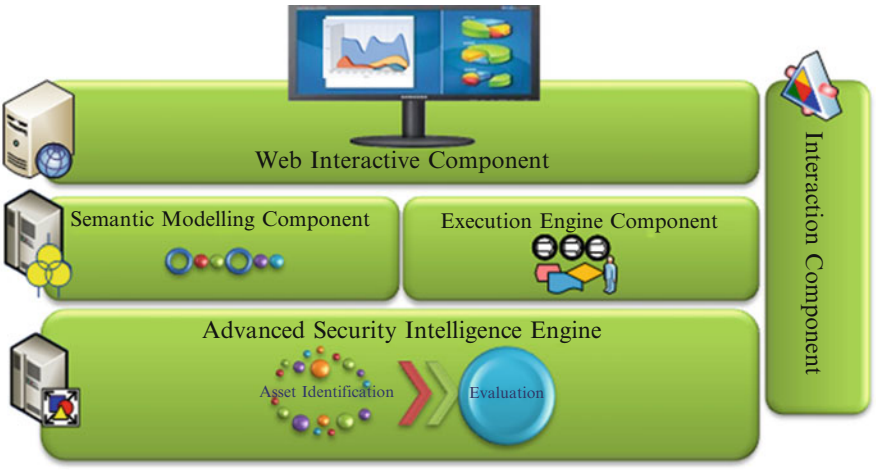


Fig. 2 CYSM system architecture

- The Semantic Modeling component that integrates a collection of semantic structures (notably ontologies/taxonomies) modeling:
  - the security and safety posture of the ports;
  - the employees of ports based on their cognitive state and behavior regarding their role and responsibilities in their enterprise, existing background knowledge about security and safety, and level of their interaction with the port infrastructure;
  - all the cyber and physical aspects (e.g., security- and safety-related legal, regulatory, and standardization framework and tools, etc.);
  - their semantic relationships providing a modularization of knowledge.
- The Execution Engine component that incorporates an automated workflow tool executes all the underlying complex processes and routines defined by the proposed CYSM Risk Management Methodology (CYSM-RM) of the services providing a high degree of automation and transparency. Also, this component undertakes the responsibility using elements of the Web Interactive component (e.g., on-line forms) to guide and direct the users to perform the required activities and actions.
- The Interaction component embodies mechanisms and interfaces that implement a set of standards and languages to encapsulate information from other services and automated tools in an automated and transparent way.
- The Advanced Security Intelligence Engine (ASIE) that delivers analysis of all activity observed within the ports' environment in an effective and efficient manner. The component incorporates the proposed CYSM Risk Management Methodology (CYSM-RM) and a set of technologies for enumerating, describing, measuring/quantifying, and encapsulating data (e.g., findings, threats and vulnerabilities metrics, and prioritization of countermeasures). With a practical combination of flexibility, usability, and comprehensive data analysis, the proposed engine delivers visibility to risks, threats, and critical operations issues. Also, it will provide full life cycle of security and safety management by incorporating the following components:
  - The Asset Identification component encompasses the mechanisms required to collect and gather the critical information and physical assets of the evaluated ports' facilities. These aspects are not confined only to technical issues, but they are also concerned with the business and physical processes in which the systems are embedded.
  - The Evaluation component integrates the appropriate means to assess the security and safety of ports' operational environment. This component conducts an analysis to pinpoint threats and vulnerabilities and assigns a rank to each based on the risk potential verses consequences. Finally, it can make recommendations on how best to minimize against these consequences.

CYSM Security Assessment Services

This section presents all different services implemented in the CYSM System. These services provide guides, guidelines, and practical advices for all ports and their employees on how to self-assess and self-organize their security issues. The main services categories encompassed in the system, depicted in Fig. 3, are as follows:

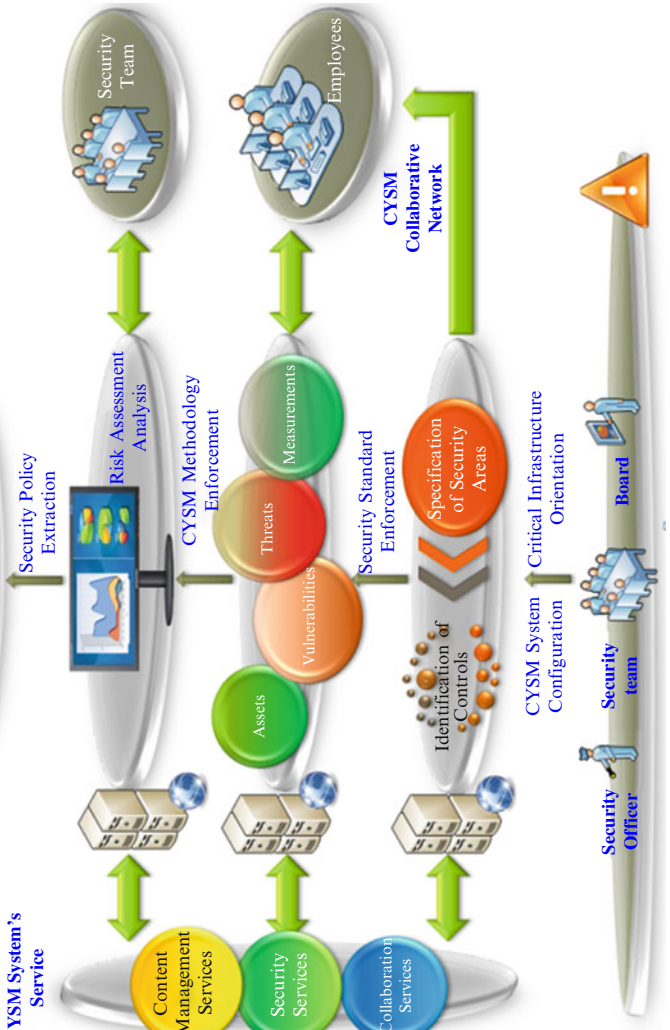


Fig. 3 CYSM system architecture CYSM security assessment services

Risk Analysis Services (RAS): The main objective of the Risk Analysis Service is to provide a straightforward and intuitive approach that can be applied by the ports covering both their security and safety issues and characteristics. The RAS gives the analysis of the cyber and/or physical problems in a unified way. It examines the overall infrastructure (ICT and/or physical) and enforces common mechanisms, procedures, and practices to provide an in-depth and accurate diagnostic of cyber and/or physical risks. The service covers all the principles of an integrated risk analysis process containing steps such as assets and threats identification, determination of impact, evaluation of threats and vulnerabilities, and determination of risks. In a nutshell, the RAS encompasses the following five-phase process:

- *Scope Definition*: defining the evaluated parts of the ICT and physical infrastructure.
- *Analysis of the assets' dependency*: identifying the cyber and physical assets of the port infrastructure and their interconnections as well.
- *Countermeasures determination*: identifying the deployed security and safety countermeasures.
- *Impact Determination*: defining the impact and the consequences of an incident to the ports infrastructures.
- *Evaluation*: identifying the threats for all assets in the ICT system (under examination) and their vulnerability levels for these threats.
- *Risk Analysis*: evaluating the risks' level.

Risk Management Services (RMS): The Risk Management Service aims to provide the guidance for the establishment, implementation, maintenances, and improvement of a common comprehensive information security and safety strategy in the ports. This strategy defines the aspects of the ports' infrastructure (ICT and/or physical elements and components) that should be improved. The service implements the main principles and activities of the risk management process defined in the CYSM Risk Assessment approach.

The RMS interacts with the RAS in order to integrate the produced results of the risk analysis process. In particular, through the RAS, the ports' users complete the identification and valuation of cyber and physical assets, the formulation of threats' profiles, the identification of infrastructure's vulnerabilities, and the evaluation of the corresponding risks in order to consume the security and safety ports' level. The assessment results are fed to the RMS, which analyses them in order to identify security requirements and possible solutions, and to detect contingency requirements and possible solutions.

In this context, the RMS proceeds with the formulation of an initial risk treatment plan. The proposed plan provides an overall strategy that will assist the ports' operators to deal with the identified physical and cyber risks taking into account requirements, rules, recommendations, controls, and particularities imposed by various security- and safety-based standards, specifications, and best practices such as ISO/IEC 27002:2005 and ISPS code.

Document Management Services (DMS): The Document Management Services provides an intuitive, interactive, and graphical way to represent and manage all the

security- and safety-related information and content (e.g., requirements, rules, obligations, recommendations, and advices of the legal, regulatory, and standardization framework and regime as well as security and safety content required for automating technical control compliance, vulnerability checking, and security measurement activities). The main categories of the DMS have as follows:

- *Security Framework Service (SFS)*: It aids the ports to define their security vision and formulate and establish the appropriate security framework. It provides a user friendly and flexible way for creating customized security and safety policies and procedures in various formats (.txt, .html, .doc, .pdf, etc.). The SFS takes into account the assessment results produced by the Security and Safety Management Services (Risk Analysis and Management Services) in order to identify and develop a draft version of security and safety policies and procedures.
- *Digital Library (DiLi)*: DiLi acts as the knowledge source of all ports' physical and cyber-related information and encompasses various elements such as Legal Repository, Standards & Methodologies, Lesson Learned Repository, and Search Engine.

Supply Chain Risk Management (MEDUSA) System

Introduction

The MEDUSA Risk Assessment system (Polemi and Kotzanikolaou 2015; Papastergiou et al. 2015b; Polemi et al. 2017) aims to systematically evaluate the security risks affecting the supply chain business partners within a Supply Chain Service (SCS). The main goal of system is to increase the preparedness of the business partners while at the same time enables the coordination of their efforts towards effectively identifying and treating their risks.

In this context, the system addresses the business partners' interactions across the SCSs during the identification and analysis of their threat scenarios, supports the assessment of the partial and overall security risks while at the same time coordinates the selection of appropriate security controls which are realistic for all business partners. In addition, Medusa (Fig. 4) allows the participants to assess the risk of the cascading threat scenarios which may be realized within a SCS. The study of the cascading scenarios takes into consideration the graph relations of a potential source of a threat as well as the business role of each business partners by utilizing weights of business importance. The system enables all the SC participants to fine-tune their security policies according to their business role in the examined SCS.

MEDUSA Architectural Components

The following figure depicts the overall architecture of the MEDUSA system that consists of four main conceptual layers: Users, Information Assets, Components,

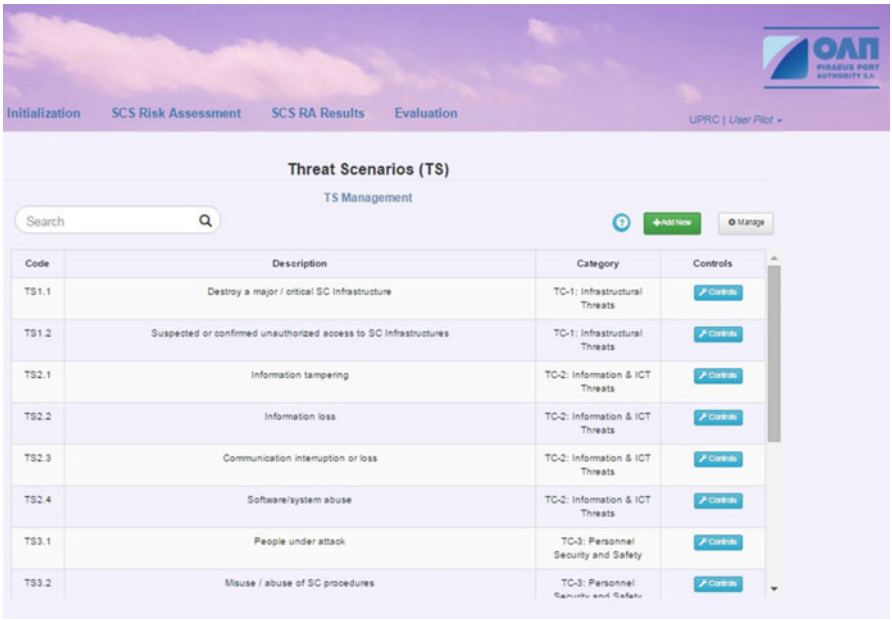


Fig. 4 Supply chain risk management (MEDUSA) system

and Technological Infrastructure. These layers constitute the conceptual pillars for building and implementing the ICT tools that will support the modeling and visualization of the various security-related risks and interdependencies.

Specifically as depicted in Fig. 5 above, MEDUSA system is composed of:

- Layer 1 – System users: MEDUSA ecosystem consists of the following user groups:
  - Security Manager: The purpose of the Security Manager is to initialize the system with information that is globally available to the other two roles. In particular, he/she has to refine and populate the closed "closed lists"/vocabularies that will be used by the other layers.
  - Supply Chain Service (SCS) Security Officer: He/she is responsible for the initiation of a risk assessment and the specification of the SCS that will be examined identifying all the involved business partners and the supported processes.
  - Business Partner Representative: The representative of a business partner (e.g., customs, insurance company, shipping company, maritime ministries, public authorities) that participate in the SCS evaluation process and provide information relating to the threats, vulnerability, and controls that belong to the area of his/her responsibility.

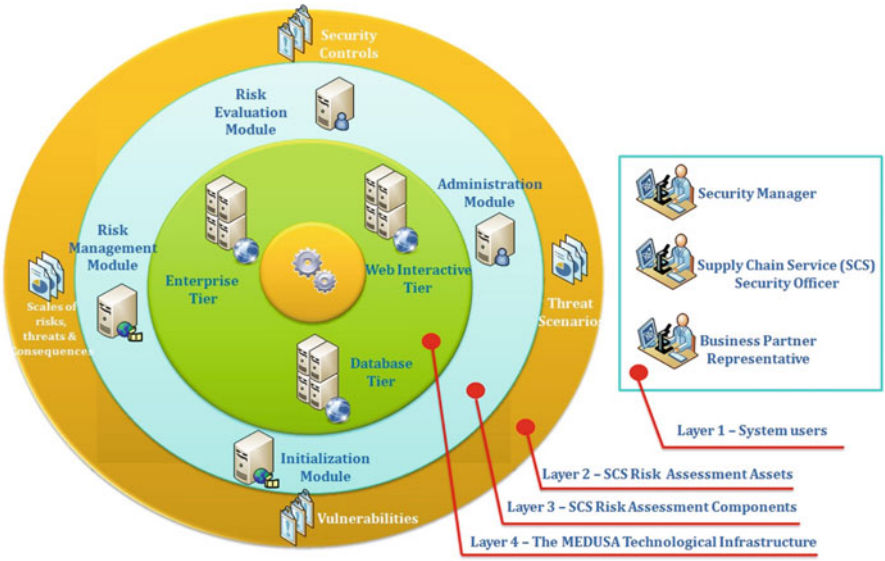


Fig. 5 MEDUSA modeling tools

These user groups are defined according to their roles, requirements, and responsibilities; therefore, they have different access rights to the components and tools of the system.

- Layer 2 – SCS Risk Assessment Information Assets: All user groups provide initial content to the system including but not limited to the following: Threat scenarios, Security Controls, Vulnerabilities, and types of Enumerations such as Types of Dependencies (e.g., access to cyber-systems and e-data, access to physical facilities), Types of Business Partners (e.g., ports, customs, importers, exporters, ship owners), Categories of Consequences, and scale of risks, threats, and consequences (e.g., High).
- Layer 3 – SCS Risk Assessment Components: All SCS Risk Assessment Assets are accessed, properly managed and processed by the implemented components. These components are:
  - Administration module: allows customizing the parameters, elements, and features (e.g., threats, vulnerabilities, controls) required for the execution of a risk assessment process based on the defined Medusa methodology.
  - Initialization module: allows the initiation of a risk assessment and the definition of the Supply Chain Service (SCS) that will be examined.
  - Risk Evaluation module: gives the opportunity to the users to assess the partial risk level of the involved business partners for the examined threat scenarios partial risk of the examined SC Service.

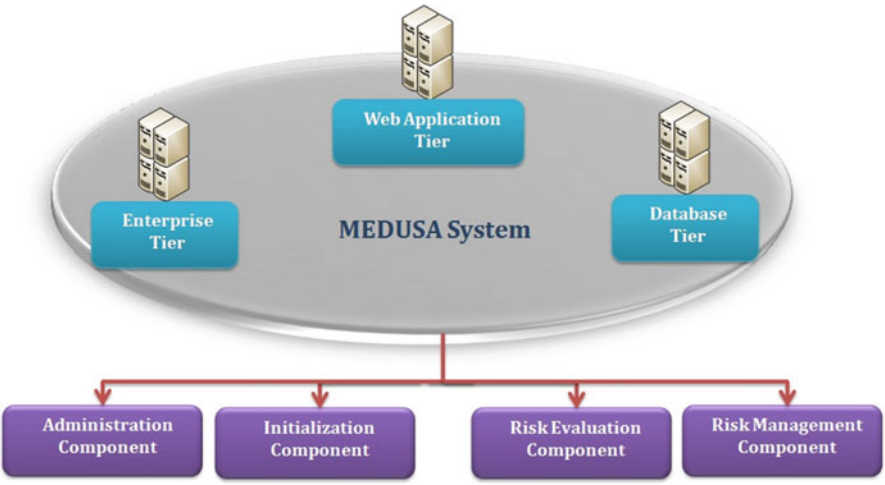


Fig. 6 MEDUSA architecture

  - Risk Management module: allows the review of the risk assessment results and the calculation of the cumulative cascading dependency risk values for the applicable threat scenarios.
- Layer 4 – The MEDUSA Technological Infrastructure: All different modules, subsystems, and primary services that comprise the MEDUSA system.

MEDUSA Architecture

The following figure (Fig. 6) depicts the architecture of MEDUSA system, illustrating all fundamental systems and technological components and modeling tools that have been implemented. The proposed system is based on an 3-tier architecture, so it is composed of the Web Interactive tier, the Application tier, and the Database tier.

The main responsibility of the Web Interactive Tier is to deploy graphical interfaces for end-users in order to represent the MEDUSA information and content and provide access to the corresponding functionalities, supporting the desired levels of simplicity, intuitiveness, and user-friendliness. As a result, this tier is highly interconnected and constantly interacts with the Enterprise Tier, which incorporates the system's business logic.

The Enterprise Tier can be considered as the most critical part of the proposed tool since it handles all the business logic of the application. From a conceptual perspective, this layer hosts a range of mechanisms, techniques, and components grouped as follows:

- The Risks, Assets, and Dependencies Modelers integrates a collection of semantic structures (notably ontologies/taxonomies) to represent the interactions,

interrelations, and dependencies in the key issues, factors, indicators required for the modeling and execution of risk management scenarios. In particular, this module implements algorithms for identifying and modeling the multiorder dependencies of the different business partners (CIIs and maritime entities, etc.), in the scope of multisector cross-border scenarios.

- The Impact Analysis and Visualization Tools embodies mechanisms, procedures, and interfaces to provide an in-depth and accurate diagnostic of various threat scenarios and security events related to the examined Supply Chain Services. These tools incorporate methods, algorithms, standards, and technologies for enumerating, describing, measuring/quantifying, and encapsulating data required by an integrated risk analysis process (such as threats identification, estimation of impact, evaluation of threats, and determination of the corresponding risks).
  In addition, these tools provide the means for a quick and visual reference to risk values. In particular, they provide a visualization approach for visually browsing the analysis results and identifying threat scenarios that are applicable to various parts of the SCSs. The visualizations are based on treemaps, graphs, histograms, etc., which greatly facilitate the exploration and identification of the relevant threats and risks.
- The Simulation Environment incorporates a set of ICT tool that undertake the responsibility to design and execute risks and threats simulation experiments that facilitate the analysis, assessment, and mitigation of various threats and risks associated with the examined SCSs. The supported functionalities of this component provide access to the simulation results for further analysis and use, as well as for the formulation of effective mitigation plans.

Finally, the Database Tier integrates the main database of MEDUSA system and undertakes the storage and management of all risk-related content and information objects.

MEDUSA Functionality

MEDUSA system aims to provide guidance to the supply chain operators on how to assess and organize the security issues associated with the SCSs in which they involved. In this context, the MEDUSA system encompasses and executes the following evaluation process that implements the main steps of the proposed Medusa Supply Chain Risk Assessment Methodology:

(a) *SCS Risk Assessments (SCS RAs) Initiation and Specification*: Specification of the boundaries of the SCS Risk Assessment such as the examined SCS, the Business Partners involved, the acceptable risk thresholds.
(b) *SCS Initiation and Specification*: Specification of the main aspects (actors involved and existing dependencies) of a Supply Chain Service.
(c) *Threat Scenario Identification*: Identification of the threat scenarios that are applicable to the SCS under examination.

(d) *Threat Analysis*: Assessment of each Threat Scenario that is relevant to the Supply Chain Service under examination by estimating its probability of occurrence the SCS.
(e) *Security Controls Declaration/Vulnerability Assessment*: Specification of the implementation level of the security controls related with the examined SCS' threat scenarios and calculation of the corresponding vulnerability values.
(f) *Consequence Assessment*: Evaluation of the worst-case consequences that the business partner may experience, if a particular Threat Scenario is realized in any node within the SC (not in particular in the same business partner).
(g) *Individual Risk Computation*: Calculation and review of the expected risk levels for all Threat Scenarios that are applicable to the SCS under examination for all business partners.
(h) *Overall Risk Computation*: Calculation and review of the overall risk levels of the SCS under examination for all examined threat scenarios.
(i) *Cascading Dependency Risk*: Identification of all possible dependency chains and calculation of the corresponding cascading dependency risk values.
(j) *Individual Risk Simulation*: Determination of the security controls that should be deployed in order to satisfy the desired risk level (acceptable threshold).

Evidence-Driven Maritime Supply Chain Risk Assessment (MITIGATE) System

Introduction

Mitigate (Papastergiou and Polemi 2017; Kalogeraki et al. 2017; Papastergiou and Polemi 2016) targets to contribute to the effective protection of the ICT-based ports Supply Chains that arises from the ICT interconnections and interdependencies of a set of maritime entities (e.g., port authorities, ministries, maritime companies, ship industry, customs agencies, maritime/insurance companies other transport Critical Information Infrastructures – CIIs (e.g., airports) and other CIIs (e.g., transport networks, energy networks, telco networks)). This is achieved by treating the resolution of the ICT maritime supply chain risks as a dynamic experimental environment that can be optimized involving all relevant maritime actors. Mitigate approach based on simulations facilitates the identification, analysis, assessment, and mitigation of the organization-wise and interdependent cyber threats, vulnerabilities, and risks.

In the literature, the analysis and evaluation of the cyber risks are based on a straightforward approach that combines a set of parameters and features such as the likelihood of a security events and the consequences of the event itself, the exploitation level of a vulnerability etc. Mitigate aims to support this approach with rational decision making. The pursuit of Mitigate is to support risk analysis with security-related information obtained from online repositories strengthening the rational analysis. Mitigate objective is to promote a more rigorous, rational approach

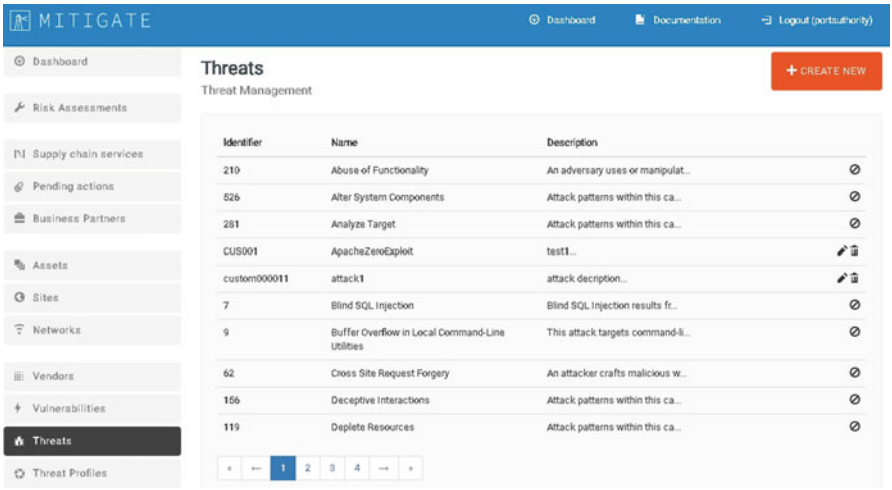


Fig. 7 Evidence-driven maritime supply chain risk assessment (MITIGATE) system

that gathers, critically appraises, and uses high-quality research information either produced by well-defined simulation experiments or are available online to enhance the risk assessment process.

In particular, Mitigate shares the view that process of evaluation and mitigation of the cyber issues is neither objective nor neutral; it should be an inherently rational process that relies on well-defined and widely acceptable security-related data and not only upon highly personalized experience, expertise, and judgment of individuals.

MITIGATE System

MITIGATE (Fig. 7) aims at realizing a radical shift in risk management for the maritime sector towards a collaborative evidence-driven Maritime Supply Chain Risk Assessment approach. To this end, MITIGATE has integrated an effective, collaborative, standards-based risk management system for port's CIIs, which shall consider all threats arising from the supply chain, including threats associated with port-CIIs interdependencies and associated cascading effects. The proposed system enables port operators to manage their security in a holistic, integrated, and cost-effective manner while at the same time producing and sharing knowledge associated with the identification, assessment, and quantification of cascading effects from the ports' supply chain. In this way, port operators are able to predict potential security risks but also to mitigate and minimize the consequences of divergent security threats and their cascading effects in the most cost-effective way that is based on information associated with simulation scenarios and data acquired from online sources and repositories (e.g., NIST Repositories).

In order for the system to meet its objectives, it has been empowered with the following features: (i) a range of reasoning, data mining, crowd-sourcing, and BigData analytics techniques that incorporate and leverage a variety of data sources and data types, enabling efficient handling of data that are incomplete, uncertain, and probabilistic; (ii) pioneering mathematical techniques for predicting and analyzing threats patterns; and innovative visualization and simulation techniques, which optimize the automatic analysis of diverse data. These ICT solutions/technologies and mathematical instruments provide a basis for implementing a variety of mechanisms and processes that facilitates collaboration between the various maritime agents enabling them to:

- Identify and model assets, processes, risks, stakeholders' relationships/interactions, and dependencies.
- Analyze threats, vulnerabilities, and countermeasures accumulated in various online sources and repositories.
- Identify, evaluate, and classify various ICT-based risks while at the same time facilitating the risk resolution.
- Design, execute, and analyze risks and threat simulation experiments in order to discover viable attack paths in the SCs. These attack paths consist of vulnerability chains that can be exploited by attackers in order to accomplish their malicious goals.
- Exploit the simulation results towards formulating effective evidence-based mitigation plans.
- Support continual Webs' vast reserve of open, distributed data uptake, integration, state assessment, decision analysis, and action assignment based on large-scale high-performance open computing infrastructures so that all agents may access and analyze a plethora of collected data and information.

MITIAGTE Overall Architecture

As already mentioned, MITIGATE system aims to provide a holistic solution regarding risk management in the frame of port supply chain services. To this end, specific set of services need to be developed and integrated in a seamless manner. Such services include assessment of risk in a collaborative manner among business partners, advanced simulation and visualization of potential attacks, and advanced reports from open intelligence analysis services. In order to achieve the goal of developing a unified system, high-level architecture has been defined and presented on Fig. 8.

As it is depicted, there are the following eight components that comprise the MITIGATE system:

- The **Asset Modeling & Visualization** component allows business partners to declare their assets along with the cyber relationships. The creation of valid asset cartography within the frame of an organization is the first step towards the

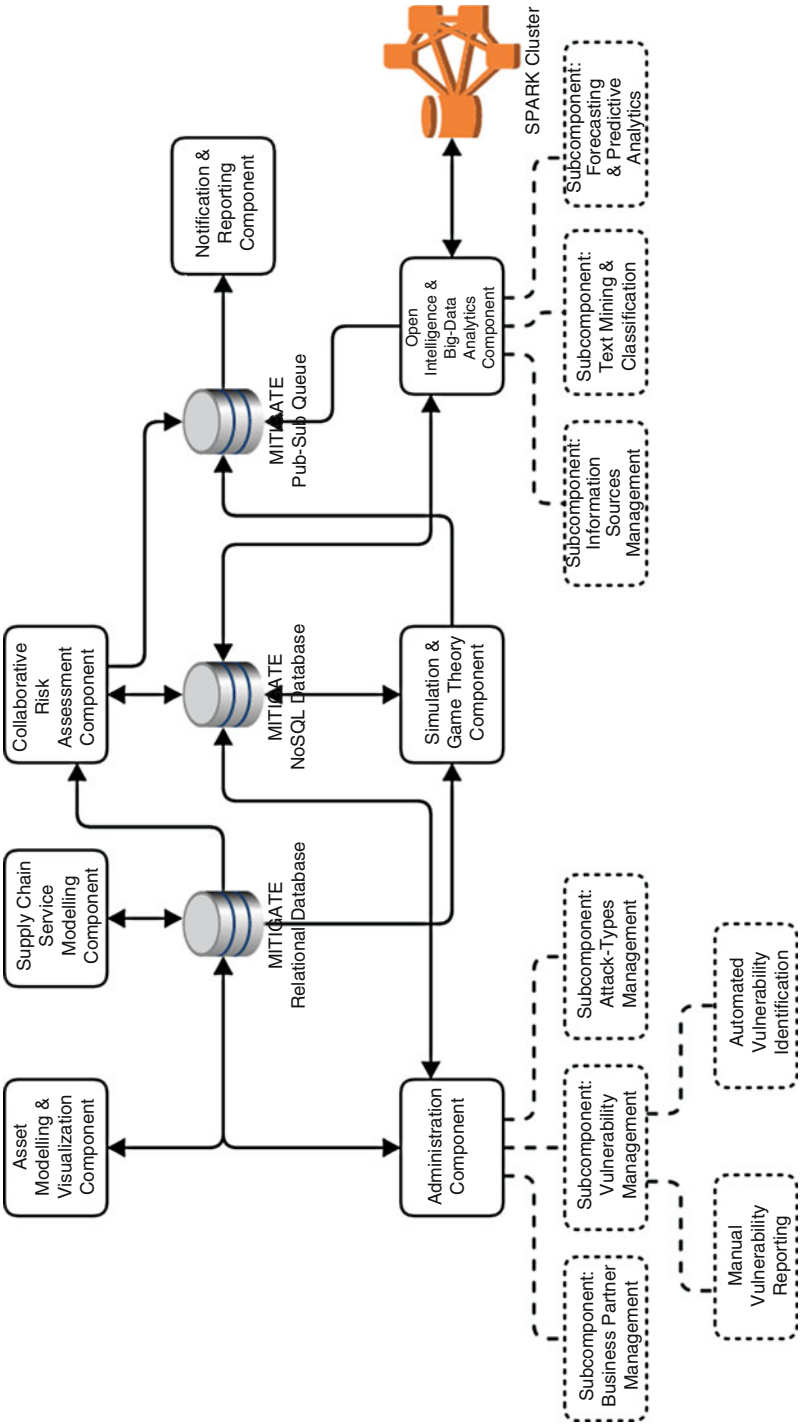


Fig. 8 MITIGATE high level architecture

realization of a collaborative risk assessment. Each organization that participates in a supply chain service will use this component in order to create its own cartography. The cartography will be automatically linked to available vulnerabilities and attack-types that are relevant to the individual assets that are declared. The cartography along with the linked information will be intuitively visualized by a graph rendering subcomponent of this component.

- The **Supply Chain Service Modeling** component allows the modeling of the examined supply chain services. More specifically, these supply chain services consist of various business processes that are performed in a synergetic way among different business partners. Each business partner has a predefined role in the supply chain service which requires the "participation" of specific cyber assets. Towards these lines, this component relies on the output of the Asset Modeling component since it allows mapping assets that are already defined in the asset cartography of each organization with the processes that these assets are involved. This "mapping" plays a significant role during the calculation of risks.
- The **Simulation & Game Theory** component has a twofold goal. On the one hand, it is responsible for the discovery of attack paths given a specific asset cartography and a specific supply chain service and on the other hand, it is responsible to propose the best defensive strategy regarding the protection of a specific asset based on game theoretical principles. Both of these features provide significant added value to the final solution.
- The **Collaborative Risk Assessment** component is responsible to provide guidance for the conduction of a risk assessment for a specific supply chain service. More specifically, MITIGATE introduced a detailed multistep processes (Papastergiou and Polemi 2017), in order to calculate the SCS-related risks. This component offers all supportive features and mechanisms that are required for an error-free execution of the proposed risk assessment methodology.
- The **Open Intelligence and Big-Data Analytics** component is responsible to provide near real-time notifications regarding potential vulnerabilities that are related to the assets that exist in the asset cartography of one organization. These notifications will be generated based on the text-processing of open sources. However, such mining techniques are extremely computational intensive; thus the component will rely on a big-data framework (SPARK) in order to achieve linear scalability.
- The **Notification and Reporting** component is responsible to provide push notifications to the business partners regarding any type of messages that are published in the pub/sub queue. Since MITIGATE involves many time-consuming operations (e.g., the conduction of a vulnerability assessment, the calculation of risks, the processing of open information sources) every time that such an operation is completed a specific message is placed in a predefined topic of the pub/sub queue. The specific component consumes all messages that relate to notification topics and presents them in a structured way to the user.

- The **Administration** component is responsible for the management and the consistency of the various "enumerations" that are required by all the other components. Such enumerations include mainly vulnerabilities, attack-types, and business partners. This component also implements the semiautomated update of these enumerations from open sources.
- The **Access Control and Privacy** component provides security guarantees in a horizontal manner to all the other components. More specifically, since the information that is provided and processed (e.g., asset cartography, attack paths, risk calculations, etc.) is extremely sensitive, the specific component undertakes the responsibility of implementing the appropriate authentication, authorization, and encryption schemes that are required in order to protect MITIGATE services and data end-to-end.

Finally, it should be noted that the architecture is complemented by a persistency layer and a pub/sub system which are totally supportive. In particular, it should be noted that the persistency layer consists of two types of databases; one relational (Mysql) and one NoSQL (MongoDB). The relational database is used in order to store fully structured data that change rarely (e.g., credentials, business partners) while the NoSQL is used in order to store semistructured data that change frequently (e.g., Vulnerability reports). The pub/sub system (ActiveMQ) is used in order to decouple the communication of the components and more specifically to eliminate any blocking communication that may be required. Elimination of blocking communication is a prerequisite for the creation of scalable system.

MITIAGTE Security Assessment Services

This section provides details regarding the main services that have been integrated in the MITIGATE system. These services include:

- The Risk Assessment and the Visualization functionalities aim to quantify the risks that derive from the various vulnerabilities associated to specific assets that participate in a Supply Chain Service (SCS). According to the proposed approach, three different qualitative risk levels are evaluated and derived. The individual risk refers to the impact of potential exploitation of several vulnerabilities at the asset-individual level. On the other hand, the cumulative and the propagated risk quantify the effect of an exploitation at a vulnerability chain level, taking under consideration that the assets which participate in a risk assessment are interconnected to each other. Cumulative risk quantifies the effect of incoming attacks to a specific asset while propagated risk quantifies the effect of an exploitation towards the adjacent network. The two latter types of functionalities raise some visualization requirements that have to be tackled.
- The Risk Management functionalities aim the generation of an optimal mitigation strategy given a specific SCS. The generation of the optimal strategy is performed

using a game-theoretic approach that takes into consideration several offensive and defensive strategies that an attacker/defender can perform on a given set of assets within a supply chain service.

- The Simulation functionalities facilitate the design, execution, and analysis of risk and threats simulation experiments that rely on a rule-based reasoning approach in order to generate the chain of sequential vulnerabilities on different assets that arise from consequential multi-steps attacks.
- The open intelligence functionalities relate to the dynamic aggregation and indexing of content that relates to cyber-security. This aggregation is achieved using crawling techniques in order to extract information from various web sources and social media regarding cyber-security aspects. The extraction and the indexing employ big-data techniques in multiple stages since the involved processes are both computationally and storage intensive.
- The prediction and forecasting functionalities provide automated identification of potential vulnerabilities and attacks in the maritime supply chain. More specifically, the indexed dataset that is crawled by the open intelligence functionalities is automatically queried based on specific keywords that are automatically extracted by the profile of assets that are registered by security officers. The automatic correlation of news with the existing assets will provide the risk assessor the possibility to register zero-day exploits and rerun the risk assessments that have been already prepared.

Evolution from CYSM to Medusa and Finally to Mitigate

With the detailed specifications of the three (CYSM, Medusa, MITIGATE) risk management system, this section outlines the objectives and targets of these approaches in ten areas revealing the evolution of results. In particular, the table lists the capabilities of CYSM, MEDUSA, and MITIGATE across various functional areas presenting the evolution from CYSM to Medusa and finally to Mitigate.

It should be noted that the MITIGATE system has been built upon the security and safety management system developed in CYSM and Medusa. However, while CYSM and MEDUSA have been the baseline infrastructures for the development of the MITIGATE system, a number of advances have also been carried out in the scope of the MITIGATE implementation and integration. In terms of ICT technologies, MITIGATE has been exploited: (a) Cloud computing for the development of the web-based service-oriented and on-demand collaborative infrastructure; (b) BigData technologies for threat analysis, including prediction and anticipation of threat and (c) Semantic web technologies (including ontologies) for the representation of assets, risk models, and assurance models, including the representation of data from open intelligence sources (i.e., social network and crowd-sourcing).

In this vein, the following table presents the evolution from CYSM to Medusa and finally to Mitigate (Table 1).

Table 1 Evolution from CYSM to Medusa and finally to Mitigate

Area	CYSM	Medusa	MITIGATE
Scope & context-boundaries	CYSM emphasizes on the protection of port facilities, based on the provision of a dynamic risk management methodology for ports' CII considering their physical-cyber nature	MEDUSA focuses on the protection of the port supply chain. It defines a methodological approach for the identification of multiorder dependencies of security risks, in the scope of multisector cross-border scenarios	MITIGATE enhances CYSM & Medusa towards protecting port facilities in the scope of interacting supply chains. MITIGATE adopts an evidence-driven maritime supply chain risk assessment model in order to capture and deal with cascading effects risks, threats, and vulnerabilities, associated with the ICT-based maritime supply chain
Threats landscape	CYSM supports identification and measurement of organization-wise threats. These include internal threats pertaining to the ports' ICT and physical infrastructure	Medusa supports identification and measurement of cross-sectoral and cross-border threats, including threats associated with cascading effects	MITIGATE supports the identification and measurement of combined cross-sectoral and cross-border attacks/threats paths and patterns arising from the ports' supply chain, both organization-wise and interdependent cyber threats deriving from the interconnection of the ports with other entities (e.g., ships, port authorities, maritime/ insurance companies, customs, ship-industry) are evaluated
Impact analysis model	CYSM is based on models that determine the value of the corporate assets and estimate the potential impact of threats in terms of specific criteria (availability, confidentiality, integrity) and based on various organizational scenarios (cost, legal, technical, . . .)	MEDUSA aims at modeling, visualizing, and simulating security scenarios and their cascading effects cross CIs that are dependent on port CIs	MITIGATE enhances CYSM and Medusa in order to perform impact analysis for threats/ assets involved in supply chain operations. This requires the integration of appropriate assurance models that are able to capture cascading effects and business factors in a multisector, multistakeholder maritime environment

(*continued*)

Table 1 (continued)

Area	CYSM	Medusa	MITIGATE
Countermeasures	CYSM introduces countermeasures for reducing ports' risks	Medusa identifies and documents security measures that could minimize the consequences of cascading effects in multisector cross-border port security scenarios	MITIGATE introduces additional countermeasures towards reducing risks associated with the whole supply chains. The countermeasures are produced based on the results of various simulation experiments, thereby exploiting the proposed evidence-based risk assessment approach
Cartography capabilities	CYSM operates on the based on the identification and representation of the ports' architectural structure	Medusa introduces algorithms for identifying multiorder dependencies between entities involved in the maritime supply chain	MITIGATE introduces algorithms and techniques for capturing and analyzing the multiorder dependencies between ports' ICT infrastructures and multiple critical information infrastructures (CIIs) participating in the global supply chain
Risk analysis	CYSM's risk analysis of the ports' facilities is based on a straightforward approach that relies only on the ports' users knowledge	MEUDSA assesses security risks, in the scope of multisector cross-border scenarios	Risk analysis in MITIGATE for the ports' supply chain is based on a more rigorous, rational approach that relies on high-quality scientific- and experimental-based data (e.g., simulation results, indicators, recommendations) and security-related information available at online repositories
Risk computational model	In CYSM a multicriteria group decision-making model has been developed and adopted in order to calculate the actual risk factor. The proposed model takes into consideration a set of criteria and	MEDUSA adopts an approach based on game theory and graph theory techniques to minimize the consequences of cascading effects in multisector cross-	MITIGATE leverages simulation models (based on game theory and graph theory techniques) combined with a multicriteria group decision-making approach in order to produce timely, accurate, objective,

(*continued*)

Table 1 (continued)

Area	CYSM	Medusa	MITIGATE
	parameters as well as the opinion of various users' groups with different vision angle	border port security scenarios	reliable, relevant, and high-quality information associated based on which the multidimensional risks will be assessed
Standards compliance	CYSM is in-line with the requirement, rules, and obligations imposed by security and safety-related standards (ISO27001, 27005, ISPS) that focus on the protection of the ports' facilities	Medusa's emphasis on the supply chain will be reflected in the provision of support for ISO28000	MITIGATE leverages and implements existing security standards (such as ISO27001, 27005, ISPS, ISO2800, ISO28001) associated with the protection of the maritime ICT-based maritime supply chain
Predictive and forecasting capabilities	CYSM evaluates a predefined list of threats associated with ports' ICT and physical infrastructures	Medusa evaluates a predefined list of threats associated with ports supply chain	MITIAGATE leverages appropriate simulation models and processes for the representation and prediction of the possible attacks/threats paths and patterns. These models are used to measure their effectiveness and applicability, as well as to and to determine the exploitation, resilience, and reliability level of ports' supply chains
Risk assessment (RA) tool	The CYSM RA tool is based on a set of interactive and collaborative technologies	MEDUSA tool is based on a set of visualization tools and techniques to model and simulating ports supply chain scenarios	The MITIGATE RA tool adapts and integrates a number of risk management components, modules, and subsystems developed in the CYSM and MEDUSA and also incorporates a set of ICT technologies, including semantic web technologies (for ontology management, context management, and profiling), cloud computing and BigData, and crowd-sourcing technologies (i.e., in order to collect and analyze open information from public resources)

Conclusions

Maritime of the modern era has become more and more dependent on cyber and physical components and technologies (such as networking, telecommunications, cloud, sensor, and SCADA technologies) to operate. This is very prominent in the case of modern port infrastructures, which tend to be highly dependent on the operation of complex ICT infrastructure and networks, information technology, and trustworthy e-maritime services in order to optimize their operations. For example, nowadays, vessel navigation and propulsion systems, cargo handling and container tracking systems at ports and on board ships, and automated processes, are all controlled using software (such as cyber-physical systems) that facilitate their smooth-running operations. The resilience of the ports' infrastructure to complex risks as well as to more sophisticated attacks is a primary requirement to guarantee their business continuity. This chapter elaborates on the functionalities and capabilities of three risk assessment systems named CYSM, MEDUSA, and MITIGATE.

CYSM system is a security management revolutionary consultation environment that is oriented to the special requirements of ports and is in accordance to the basic principles and the business goals of existing risk assessment standards and methodologies. The nature of the system is associated with a high degree of innovation since it implements new upgrading security and safety self-management functions and processes for the evaluation and mitigation of the risks and threats associated to the ports' infrastructure. The CYSM system has been tested and evaluated by a number of commercial ports (including Port of Piraeus, Valencia Port Authority, and Port of Mykonos). During the evaluation operation, more than 283 port operators, stakeholders, and individuals (e.g., Port Security Officers, Members of Ports' Security Teams, Ports administrators, and internal users interacting with ports' ICT systems) were engaged in risk identification, assessment, and mitigation based on the on-line services of the CYSM system.

Nevertheless, it should be noted the risk assessment approach produced in the CYSM project is limited to the port's domain and do not consider or predict cross-sectoral, cross-border threats from the port's supply chains. To this direction, the MEDUSA project has introduced an innovative, scalable Risk Assessment environment which adopts a set of flexible and configurable functions and processes for building a solution that facilitates the effective and efficient evaluation of various threat scenarios associated with the MLoSCs as well as the estimation and remediation of their possible consequences. This system has been tested and evaluated by a large number of Supply Chain stakeholders as well as individuals (such as Port operators, Ports' Security Officers, government officials, leading experts from the Maritime, Oil, and Gas sector, IT professionals, and Security and risk management experts) engaged in the process of evaluating the capacity of the Medusa methodology and system (http://medusascsra.cs.unipi.gr/) to meet their objectives. In particular, more than 400 port operators, government officials, leading experts from the Maritime, Oil, and Gas sector, and IT security professionals trained on the functionality and services of the MEDUSA system (including representatives from Valencia port Foundation, Port Authorities of Alicante and Castellon and Piraeus Port

Authority) and about 123 of them have used the system to identify and assess the threat scenarios and risks associated with the SCSs in which their organization participate.

However, the emerging landscape of ICT-empowered MLoSC requires a paradigm shift in the way it assesses risks and vulnerabilities, as well as in relevant risk management methodologies. For example, MEDUSA approach cannot be considered as an IT-oriented risk assessment methodology since it does not support an integrated and effective security management, evaluation, and mitigation of IT-based risks; actually it is a supply chain risk assessment methodology at organizational level. Thus, there is a clear need for rethinking risk management in the MLoSC. To this end, sophisticated global risk assessment frameworks that can deal with cascading effects risks, threats, and vulnerabilities of ICT-based maritime supply chain are needed since now the maritime industry is becoming more vulnerable to the activities of hackers and other perpetrators of cyber-related crime. In this vein, the MITIGATE project presents a risk assessment approach that enhances the protection and security of the ICT MLoSC and guarantees the continuity and the development of maritime transportation. The evaluation of the proposed system has be conducted by a number of MLoSC entities such as Piraeus Port Authority, Valencia Port Authority, Port of Ravenna, DBH Logistics IT AG, Livorno Port Authority (LPA), and Port of Bremen.

Acknowledgments This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653212, project MITIGATE . The authors also thank all partners of these projects. Finally, special thanks to University of Piraeus, Research Center for its continuous support.

References

Austrian Standards Institute. (2004). ONR 49000: Risikomanagement für Organisationen und Systeme: Begriffe und Grundlagen, Wien.

Bundesamt für Sicherheit in der Informationstechnik. (2013). IT-Grundschutz Kataloge. Online: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

CCRA Working Group. (2006). Common criteria for information technology security evaluation, CCRA. [Online] Available: www.commoncriteriaportal.org

Common Criteria Working Group. (2007). Common methodology for information technology security evaluation – Evaluation methodology, CCMB-2007-09-004. http://www.commoncriteriaportal.org

European Commission. (2004). Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security. Off J Eur Union, L 129/6, pp. 6–91.

European Network and Information Security Agency. (2010). Inventory of risk management/risk assessment methods. [Online] Available: http://rm-inv.enisa.europa.eu/rm_ra_methods.html

International Maritime Organisation. (2004). International Ship and Port Facility Security Code, London.

International Standardization Organization. (2005). ISO 20000: Information technology service management, Geneva.

International Standardization Organization. (2007). Ships and marine technology – Maritime port facility security assessments and security plan development, Geneva.
International Standardization Organization. (2009a). ISO 31000: Risk management – Principles and guidelines, Geneva.
International Standardization Organization. (2009b). ISO 31010: Risk management – Risk assessment techniques, Geneva.
International Standardization Organization. (2011). ISO 27005: Information security risk management, Geneva.
International Standardization Organization. (2013). ISO 27001: Information security management system requirements, Geneva.
Kalogeraki, E. M., Polemi, N., Papastergiou, S., & Panayiotopoulos, T. (2017). Modeling SCADA attacks. World conference on smart trends in systems, security and sustainability (WS4 2017), Springer Computer Science proceedings, 15–16 Feb 2017, London.
Karantjias, A., Polemi, D., & Papastergiou, S. (2014). Advanced security management system for critical infrastructures. Special session on "secure and sustainable maritime digital environment" within the fifth international conference on information, intelligence, systems and applications (IISA 2014), 07 July 2014, Chania Crete.
Papastergiou, S., & Polemi, D. (2014). Harmonizing commercial port security practices & procedures in Mediterranean Basin. Special session on "secure and sustainable maritime digital environment" within the fifth international conference on information, intelligence, systems and applications (IISA 2014), 07 July 2014, Chania Crete.
Papastergiou, S., & Polemi, D. (2016). Securing maritime logistics and supply chain: The Medusa and MITIGATE approaches. 1st NMIOTC conference on cyber security in the maritime environment, NATO Maritime Interdiction Operational Training Centre, 4–5 Oct 2016, Chania Crete.
Papastergiou, S., & Polemi, D. (2017). MITIGATE: A dynamic supply chain cyber risk assessment methodology. World conference on smart trends in systems, security and sustainability (WS4 2017), Springer Computer Science proceedings, 15–16 Feb 2017, London.
Papastergiou, S., Polemi, N., & Karantjias, A. (2015a). CYSM: An innovative physical/cyber security management system for ports. Third international conference, HAS 2015, held as part of HCI International 2015, Los Angeles, CA, 2–7 Aug 2015. Proceedings, pp. 219–230.
Papastergiou, S., Polemi, D., & Papagiannopoulos, I. (2015b). Business and threat analysis of ports' supply chain services. Special session on "innovative risk management methodologies and tools for critical information infrastructures (CII)" within the 6th international conference on digital human modeling and applications in health, safety, ergonomics and risk management (HCI International 2015), 2–7 Aug 2015, Los Angeles, CA.
Peltier, T. R. (2001). *Information security risk analysis*. Boca Raton: Auerbach Publications.
Polemi, N., & Kotzanikolaou, P. (2015). Medusa: A supply chain risk assessment methodology. *In Cyber security and privacy: Vol. 530. Communications in computer and information science*. Cham: Springer
Polemi, D., & Papastergiou, S. (2015) Current efforts in ports and supply chains risk assessment. IEEE proceedings of the 10th international conference for internet technologies and secure transactions, London.
Polemi, N., Kotzanikolaou, P., & Papastergiou, S. (2017). Design and validation of the MEDUSA supply chain risk assessment methodology and system. *International Journal of Critical Infrastructures*. Inderscience Publishers (Status: Under review).
S. E. Schechter. (2004). Computer security strength and risk: A quantitative approach, Harvard University, Cambridge, MA.
The Stationery Office (TSO). (2007). Continual service improvement, ITIL V3.

Cyber-Security Policies of East European Countries

48

Dusko Tomic, Eldar Saljic, and Danilo Cupic

Contents

Abstract

In modern times, ensuring security in cyberspace is the main task of national security for most states. States have different approaches to cybersecurity from the aspect of national security policies. They can be divided into two categories: those that regard cybersecurity as a civilian task and those that involve their

D. Tomic (✉) · E. Saljic
American University in the Emirates, Dubai, UAE
e-mail: dusko.tomic@aue.ae; eldar.saljic@aue.ae

D. Cupic
Ministry of Internal Affairs, Podgorica, Montenegro

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_59

militaries in creating or implementing cybersecurity policies. Those states that have incorporated cyber warfare into their military planning and organization perceive cyberattacks as a threat to their national security, while states that charge their civilian agencies with domestic cybersecurity missions classify cyber intrusions as security risks for only particular sectors. Adopting the framework of securitization theory, this chapter theorizes both civil and military approaches to cybersecurity and threat perceptions and their sources. The theoretical framework is then applied to a study of the cybersecurity policies of Eastern European countries and the Baltic states.

Keywords
Cybersecurity · Cyber space · National security

Introduction

Today, cybersecurity is increasingly regarded as a national issue affecting all levels of society (ENISA 2012). Consequently, securing cyberspace has become an integral part of states' national security policies. Cyber threats have revolutionized the way people think about security and the rules and methods for safeguarding national security (Świątkowska 2012). Although, defining cyber threats seems to be problematic, almost all states agree that cyberspace threats and risks need to be specifically addressed in their national security policies. It is ever so common that low level of national security can cause terrorism to arise and that terrorism can also have a significant impact on the cybersecurity of a state, as Saljic et al. have stated in their article regarding terrorism and security, where they considered that terrorism embraces new forms and gains new contents (Saljic et al. 2004). Furthermore, another paper states that transitional countries need to work on better cooperation in the fight of the contemporary forms of crime (Šaljić and Đorđević 2011). Countries around the world are, therefore, formulating cybersecurity strategies, usually by devising some kind of national legal act or program to respond to cyber threats and protect critical networks (the Cyber Index, UNIDIR 2013). However, priorities for national cybersecurity policies vary by country. Some countries have a very clear vision of the cyber environment and its main referent objects such as critical infrastructure (*CI*), have formulated a comprehensive perception of issues that pose threats to cybersecurity and national security, and have identified the most dangerous source of cyber threats. As a result, in these countries, tasking government agencies with cybersecurity management is a key condition for implementing effective cybersecurity policies. In contrast, states with a prevailing civil approach to cybersecurity are mainly concerned with cybercrime. The potential sources of cybercrime risks are more diffused and primarily related to private property and the proper functioning of the economic sector.

The roots of states' different approaches to cybersecurity can be analyzed from a theoretical point of view. There are competing doctrines for viewing cybersecurity

issues. The so-called national security paradigm reflects the traditional role of the state in securing countries' borders and enforcing the rule of law (Newmeyer 2015). According to Harknett and Stever (2009), the cybersecurity issue is a unique multifaceted, establishing cybersecurity that requires states to secure public, private, and economic cyber activities. Cybersecurity is considered fundamental to a state's military and economic security and as such is approached with traditional national security arguments based on protecting the homeland (Harknett and Stever 2009). In other words, this approach emphasizes the link between the protection of critical infrastructure and those public and private systems that are important to the operation of the government. The national security paradigm refers to the top-down approach of managing and securing cyberspace risks in a manner that may result in increasing the military's influence on cyberspace policies (Dunn Cavelty 2013). Therefore, the concept of cyberspace militarization can be analyzed through the national security paradigm.

In contrast to the military approach, the civil approach can be analyzed through an economic lens. In this regard, the economic paradigm reflects the growing influence of the internet on the state's economic well-being (Newmeyer 2015). While the national security paradigm excludes all other sectors but the military from the processes of formulating cyberspace policies, the economic perspective emphasizes the importance of the participation of other sectors and institutions in the formulation of cybersecurity policies. According to Moore (2010), from the economic perspective, there are two necessary conditions to implementing a national cybersecurity strategy: (1) internet service providers should be held accountable for eliminating malware-infected computers on their systems; and (2) companies and other agencies should be required to disclose data breeches and control system intrusions. The economic paradigm refers to a decentralized approach among a group of agencies and actors responsible for cybersecurity management. In this approach, the burden of taking measures to protect systems as a whole is shared by the individual, service providers, and the government.

Both paradigms, national security and economic, suggest frameworks for a theoretical analysis of the process of creating and implementing cybersecurity policies. A variety of optional theoretical approaches could still be highlighted. The framework used in this paper is the securitization framework of the Copenhagen school. As Hansen and Nissenbaum note (2009), the understanding of security as a discursive modality with a particular rhetorical structure and political effect renders the Copenhagen school's framework well suited to a study of the formation and evolution of cybersecurity discourse. Therefore, this chapter – based on the results of a qualitative study of the four Visegrad states (Poland, the Czech Republic, Slovakia, and Hungary) and the three Baltic states (Lithuania, Latvia, and Estonia) – aims to (1) investigate how the civil and military approaches correlate to securitization processes and (2) contribute to understandings of differences in states' cyberspace behaviors and cooperation patterns in cyberspace.

The Copenhagen School and Cybersecurity

In the 1990s, securitization theorists such as Buzan, Weaver, and De Wilde did not perceive cybersecurity as an existential threat to states. However, as a consequence of the growing dependence of human societies on cyber networks, cybernetic issues are now securitized, suggesting that the materialization of this process is highlighted through an analysis of policies and institutional and strategic responses (Lobato 2015). Thus, it is important to analyze how states, acting as securitizing actors, become alert to the risks of cyberattacks and then establish a specific agenda to deal with threats. In this context, maintaining a secure cyberspace legitimizes the use of extraordinary measures. The ability of an actor to successfully securitize an issue is highly dependent on their position. According to Buzan, security has, to some degree, been institutionalized, and, therefore, "some actors are placed in positions of power by virtue of being generally accepted voices of security, by having the power to define security" (Buzan et al. 1998). A government's cybersecurity policy would therefore seem to be an ideal vehicle for mobilizing, and perhaps also legitimizing, a securitizing move. A policy represents an administration's official stance on an issue understood to be a problem and proposes solutions based on technical knowledge and research. In this regard, cybersecurity policies reflect in strategic documents, such as the national and cybersecurity strategies, the processes of defining cyberspace as a realm requiring security measures.

Given this, I operationalize both military and civil approaches of cybersecurity in order to apply the Copenhagen school's theoretical framework to my cybersecurity analysis. Thus, in countries with a military approach, the referent object is the protection of critical infrastructures and of governmental digital resources. Countries implementing this approach are usually technologically advanced, have larger economies, and rely heavily on cyberspace. With this dependency comes vulnerability and maintaining critical cyber infrastructure that is considered the main condition for maintaining national security. Conversely, there is no specific referent object identified by civil-oriented countries. These countries believe that cyberattackers are seeking immediate financial gain or seek to steal sensitive or provocative information. Since cyber threats are closely linked to criminal acts, the main referent object varies from personal information to the proper functioning of information, economic, and social spheres and other so-called soft sectors.

The second point made by the Copenhagen school is that the concept of security encompasses not only military, but also political, economic, and social aspects. Consequently, the *perception of threats* has also been expanded. Hence, in this chapter, it is important to analyze how countries perceive potential cyberattacks. Thus, states with a prevailing military approach – due to their heavy dependence on their *CI* – view cyber issues as matters of national security and include cyber warfare in their military planning and organization. It is worth mentioning that dimensions of national cybersecurity were established when computer intrusions (a criminal act) were clustered together with more traditional and well-established espionage discourse. In this regard, civil-oriented countries perceive particular cyber issues as security risks for only a particular sector, such as financial, social, or private spheres.

Table 1 Presumptions of military and civil approaches

Civil approach	Military approach	
Referent security object	Private security, information and communications technology (ICT)	Critical infrastructure, ICT
Cyberattack perception		National security threats
Sources of cyber threats	Criminal acts, security risks	Rogue states and non-state actors, cybercriminals, hacktivists
	Non-state actors, cybercriminals, hacktivists	
Institutions responsible for cybersecurity management	Interior ministries and civil agencies, etc.	Ministries of defense, other military agencies

According to the Copenhagen school, security discourse refers to the identification of the main *source of threat*. Although, the architecture of cyberspace makes it difficult to clearly determine who initiated a cyberattack, the military approach usually focuses on foreign governments and rogue non-state actors as the sources of threat, while the civil approach concentrates on hacktivism and cybercrimes as the main sources of threat. Consequently, countries with a prevailing civil approach are less likely to envision external threats to cybersecurity. The actors posing the greatest threats in countries with a civil approach may be in the business of stealing personal identities to commit fraud, a crime that in the interconnected world of cyberspace renders everyone a potential victim.

Another stage of the securitization process is the acceptance and legitimization of the *extraordinary measures* offered by the securitizing actor. Therefore, based on this logic, the active engagement of military institutions in cybersecurity policy creation and implementation could be seen as one such extraordinary measure undertaken by countries with a prevailing military approach. The so-called militarization of cyberspace refers to the growing pressures on governments to develop the capacity to fight and win wars in this domain (Deibert 2011). Therefore, the militarization of cyberspace shall be considered a result of the securitization process. When cyberspace is perceived as a source of threats to national security, governments strengthen their capabilities to offensively fight these threats. Meanwhile, civil-oriented countries are more likely to respond to perceived cybersecurity threats with civilian capacities, structures, and instruments as cybersecurity issues ultimately fall within the remit of interior ministries and civilian agencies.

While cyberspace is not specifically addressed by Buzan et al. the securitization theory could serve as the theoretical framework for the analysis of civil and military approaches to cybersecurity; their relevant premises are demonstrated in Table 1.

Overview of Cybersecurity Strategies and the Institutional Structuring of Cybersecurity Policies

In the hierarchy of strategic documents, cybersecurity strategies are part of the national security or defense strategies and are connected to several other institutions' strategies due to the all-encompassing impact of cybersecurity on society as a whole.

The main goal of this section is to provide an overview of cybersecurity strategies of seven selected countries and the institutions engaged in the implementation of cyber policy objectives.

Estonia

Estonia's strategic documents on cybersecurity and its institutional structures for maintaining cybersecurity have contributed to its mature and comprehensive cybersecurity culture and policies. This is a country where strategic planning comes first, ensuring the cohesion of the entire cybersecurity architecture. In response to a series of extensive hacking attacks in 2007, Estonia, in 2008, became one of the first countries in the world to adopt a national cybersecurity strategy. The hacking episode Estonia faced in 2007 has been called the first cyberwar, raged as a politically motivated assault, on a country's digital infrastructure. After this "Cyber War I," Estonia's Ministry of Defense drafted a national cybersecurity strategy. Estonia has also published and launched *Digital Agenda 2020* to create an environment facilitating the use of ICT and the development of smart solutions (Digital Agenda 2020 for Estonia, 2013).

Estonia has the most extensive range of institutional cybersecurity policies in the Baltics. The responsibility for coordinating Estonia's cybersecurity policies overall was transferred from Estonia's Ministry of Defense (MOD) to its Ministry of Economic Affairs and Communications in 2011. As an interagency body, Estonia's Cyber Security Council of the Security Committee of the Government has been supporting strategic level interagency cooperation and overseeing the implementation of the country's cybersecurity strategy objectives. The Ministry of Defense is the coordinating authority for cyber defense in the area of national defense. In addition to the MOD, national cyber defense is supported by the Estonian Defense League Cyber Defense Unit that includes cybersecurity professionals from both the public and private entities. Since 2008, Estonia's defense forces have also hosted the NATO Cooperative Cyber Defense Centre of Excellence – an international military organization focusing on enhancing the cyber defense capabilities of NATO and its sponsoring nations.

Latvia

The *Cyber Security Strategy of Latvia for 2014–2018* was adopted in 2014 (Cyber Security Strategy of Latvia 2014–2018, 2014). The strategy highlights the ICT security incidents in Latvian cyberspace and predicts that the country may be subject to increased cybersecurity risks in the future (Cyber Security Strategy of Latvia 2014–2018: 2014). The strategy also appeals to the *Law on the Security of Information Technology* which determines basic security requirements for state, municipal institutions, and providers of public electronic communications services, as well as supervisors of critical ICT infrastructure. Both documents reflect an integrated

approach to the protection of Latvia's cybersecurity and national security that prioritizes critical infrastructure and public services.

Latvia's elaborate and efficient institutionalization of its cybersecurity policies is well on the way to becoming a model system. Latvia's National Information Technology Security Council coordinates the development of national cybersecurity policies and the implementation of the policies' objectives and measures. The Council is the central national authority for the exchange of information and cooperation between the public and private sector and the Ministry of Defense coordinates the development and implementation of information technology security and cyberspace protection policies. Naturally, there are some other entities – such as other ministries and a computer emergency response team (CERT) – that also implement Latvia's cybersecurity policies.

Lithuania

Lithuania's management of cybersecurity threats has gone through a long evolution, starting from the creation of Lithuania's first institutions for dealing with cybersecurity to the recent passing of an overarching law on cybersecurity (Butrimas 2015). Lithuania is the only country in the Baltic region that has not approved a national cybersecurity strategy. However, Lithuania's Seimas (parliament) approved a national security strategy, which declared cybersecurity a priority of national interest. In order to ensure the security of Lithuania's cyberspace, the Lithuanian government approved *The Programme for the Development of Electronic Information Security for 2011–2019*. The program has three main objectives: (1) to strengthen the security of state-owned information resources, (2) to ensure that critical information infrastructure functions efficiently, and (3) to ensure the cybersecurity of Lithuania's citizens and residents and persons staying in Lithuania (Resolution Nr. 796, 2011). These objectives have been carried over to and further developed by Lithuania's law on cybersecurity, approved in 2014. The significant outcomes of this law include transferring of coordinating national cybersecurity policies to the Ministry of National Defense (MoND), the establishment of a new operational National Cybersecurity Center (NCC), and the creation of an Advisory Council on Cybersecurity chaired by the MoND (Law on Cyber Security of the Republic of Lithuania, 2014).

Poland

Poland enacted a long list of comprehensive changes to its cyberspace defense system and managed to publish and implement a cybersecurity strategy. Furthermore, cybersecurity also became an integral part of Poland's national security efforts and is frequently mentioned in other national strategic documents.

The cybersecurity issue in Poland's strategic documents was first mentioned in the *National Security Strategy of the Republic of Poland* in 2007. The document noted a direct relationship between cybersecurity and the country's ability to

function properly (National Security Strategy of the Republic of Poland, 2007). Later, the *Strategy of Development of the National Security System of the Republic of Poland 2011–2022* detailed and developed the issues related to cyberspace protection in Poland (the Strategy of National Security of Poland, 2012). However, the first document dedicated solely to cybersecurity, *Cyberspace Protection Policy*, was not published until 2013 (Cyberspace Protection Policy of the Republic of Poland, 2013). In 2015, Poland's National Security Bureau (BBN) published a cybersecurity doctrine (Świątkowska 2012). The document further lays out work to be completed in order to improve national security in the realm of cyberspace. The doctrine also maps out tasks for state institutions, notably for security agencies, the armed forces, the private sector, and NGOs (Doctrine of Cybersecurity of Poland, 2015). The National Security Bureau, functions as the main entity – together with the Ministry of Administration and Digitization, the Internal Security Agency, and CERT – responsible for achieving cybersecurity objectives.

The Czech Republic

The Czech National Strategy for Information Security approved in 2005 marks the Czech Republic's first attempt to regulate its national cyberspace (National Strategy for Information Security in the Slovak Republic, 2005). In 2011, the National Security Strategy identified cybersecurity as one of the main priorities of the Czech government and placed cyber threats on the same security-threat level as regional conflicts, terrorism, and weapons of mass destruction (Security Strategy of the Czech Republic, 2011). In 2011 the Czech Republic approved its cybersecurity strategy and action plan for 2011–2015. The strategy primarily aimed to protect ICT systems in the Czech Republic and mitigate damage caused by cyberattacks (Cyber Security Strategy of the Czech Republic for years 2011–2015, 2011). In 2015, the Czech government approved its updated national cybersecurity strategy for 2015–2020. This strategy for the latter half of the decade includes a comprehensive set of measures that for achieving the highest possible level of cybersecurity (National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020, 2015).

In the Czech Republic, civilian agencies are charged with implementing cybersecurity policy. The overall responsibility for national cybersecurity rests with the country's National Security Authority. The National Cyber Security Center, an agency within the National Security Authority, is part of the country's national and international early warning system. Additionally, the Ministry of the Interior promotes cybersecurity issues at the political level, while the Ministry of Defense only addresses cybersecurity issues cooperatively with NATO.

Slovakia

Slovakia developed a legal framework for cybersecurity in 2008 by adopting the *National Strategy for Information Security of the Slovak Republic* (NSIS) for

2009–2013. The strategy was drafted by the Ministry of Finance, Slovakia's agency responsible for securing unclassified public administration information. In 2012, Slovakia launched its *National Cybersecurity Strategy*. The strategy was accompanied by the action plan, a report on the tasks of the NSIS. Slovakia issued an information security plan for each year from 2009 to 2013.

Slovakia's National Security Authority manages classified information, while the Ministry of Finance manages the rest. Mutual communication is facilitated by the Ministry of Finance's Committee for Information Security, which has an advisory and coordinating role, preparing strategic and technical materials on information security. Some specific topics are supervised by the Security Council, the Ministry of Interior, and the Ministry of Defense. Thus, the Ministry of Defense does not have a direct role in national cybersecurity management.

Hungary

In 2013, Hungary adopted a national cybersecurity strategy which expressly states that protecting Hungary's sovereignty in Hungarian cyberspace is a national interest (Government Decision on the National Cyber Security Strategy of Hungary, 2013). Being aware of the fact that threats and attacks emerging in cyberspace may escalate to a level requiring allied cooperation, Hungary considers it highly important that cybersecurity has become an issue for a collective defense under Article 5 of the founding treaty of NATO. It is also worthwhile to note that cyber threats are also prioritized in Hungary's national security strategy adopted in 2012 (Government Decree on the Hungary's National Security Strategy, 2012).

The main agency responsible for the coordination and implementation of cyber-related policies in Hungary is the National Cybersecurity Coordination Council. Additional institutions charged with aspects of cybersecurity: the Cybersecurity Authority (an agency within the Ministry of National Development), the National Security Office (an agency within) the Ministry of Public Administration and Justice, and CERT (an agency within).

Ukraine

In response to large-scale attacks to its critical infrastructure in recent years, Ukraine adopted in 2016 a National Cybersecurity Strategy and is making strides in its implementation. The setup of the National Cybersecurity Coordination Center in 2016 and the proposed update of the cybercrime legislation to meet the Budapest Convention requirements and best practice particularly on internet service providers are two main steps in enhancing the country's cyber resilience.

Increased digitalization of services and reliance to the internet have brought about the evolution of cyberspace, raising also significant security challenges to governments across the globe vis-a-vis offenses against and by means of computer systems. In Ukraine this has been demonstrated most significantly with the large-scale

cyberattacks to Ukrainian power companies in December 2015 following attacks to major Ukrainian TV channels 2 months earlier on the day of local elections.

These incidents fit within the overall trend that Ukraine is witnessing the past years with an increased use of distributed denial of service attacks as well as zero-day vulnerabilities exploited to penetrate and compromise critical infrastructures. The threat landscape analysis also points to targeted attacks on diplomats, law enforcement agencies, defense actors, state enterprises, mass media, as well as politicians and public figures, as well as misinformation campaigns over the Internet to influence the "physical" world.

The national cybersecurity system put in place by the strategy ensures collaboration between all government agencies, local authorities, military units, law enforcement agencies, research and educational institutions, civil groups, businesses, and organizations, irrespective of their form of ownership, that deal with electronic communications and information security or are owners of critical information infrastructure.

Cybersecurity Strategies in the Region Overall

This overview of the national cybersecurity strategies in the seven countries examined reveals that the region's cybersecurity strategies are becoming integrated and comprehensive. The strategies approach cybersecurity in a holistic manner and encompass economic, social, legal, law enforcement, military, and intelligence-related aspects of cybersecurity. Some strategies, such as those implemented in Slovakia and the Czech Republic, support a more flexible approach and emphasize the economic and personal (individual) dimensions of cybersecurity policy. Moreover, the Czech Republic, Slovakia, and Hungary belong to a group of countries where civilian agencies are mainly in charge of ensuring cybersecurity. In this regard, cybersecurity in these countries can be described as civil-oriented. Military agencies are more active in coordinating and implementing cybersecurity policies in Estonia, Lithuania, Latvia, and Poland.

Cybersecurity and Its Referent Objects

When using a securitization framework to analyze cyberspace defense, the referent object – that which is existentially threatened – is critical infrastructure. However, as Deibert and Saco have argued, cybersecurity is a terrain on which multiple discourses and (in) securities compete (Deibert 2002; Saco 1999). Therefore, discussions of cybersecurity hinge on competing ideas regarding cybersecurity's referent objects (Hansen and Nissenbaum 2009). According to Hansen and Nissenbaum (2009: 1161), the key to understanding the potential magnitude of cyber threats lies in acknowledging and understanding just how highly networked and integrated computer systems have become. These networks provide critical digital infrastructure: they regulate electricity, financial activities, energy use, and even traffic

patterns. These networks are identified as a collective referent object and are usually securitized first, since their damage would present a threat to national security.

The economic sector is also rich in referent objects including the private sector's fear of hackers' abilities to steal large sums of money and intellectual property owners' worries that file sharing compromises their rights and revenues (Hansen and Nissenbaum 2009). In this regard, an individual approach to cybersecurity – stemming from cyber-libertarianism prioritizing personal (or individual) security – prevails.1 As Hansen and Nissenbaum (2009: 1163) have argued, in private security discourse, the individual is not a referent object, instead the individual is linked to societal and political referent objects. In other words, cyber privacy defense has to be mediated through a collective referent object, either a political-ideological one – prompting questions regarding an appropriate individual-state balance – or a national-societal one, which would mobilize values core to community identity. Similarly, securing critical infrastructure cannot stop at the infrastructure itself; the implications of a network breakdown imply other referent objects: society, the regime, and the economy (Hansen and Nissenbaum 2009). In order to link a theoretical perspective on the variety of referent objects with a study of cybersecurity in the Baltic States and Visegrad countries, it requires an analysis of the referent objects identified by the states themselves.

All seven countries acknowledge a link between the cyber- and national security sectors and are aware that cybersecurity issues – such as the destruction of the ICT system or critical infrastructure – can damage national security, diversely impact citizens' lives, and threaten the assets and the proper functioning of the national economy and public services. Consequently, a collective security discourse prevails in all seven countries' strategic documents. However, the countries – such as Estonia, Poland, Latvia, Lithuania, and, to some degree, the Czech Republic – that articulate a strong need to intensively defend their cyberspaces also present, as reflected in their strategic documents, more comprehensive and clearer visions of their main referent objects. For instance, Lithuania's national security strategy emphasizes the importance of ensuring the security of informational, economic, and social infrastructure as the key objective of national security policy (National Security Strategy of the Republic of Lithuania, 2012). Meanwhile, the national cybersecurity strategy of the Czech Republic mainly prioritizes the protection of information infrastructure essential to Czech economic and social interests (Cyber Security Strategy of the Czech Republic for years 2011–2015, 2011); it also focuses on the protection of rights of internet users. However, the Czech Republic's national security strategy presents a more comprehensive concept of critical infrastructure and its vulnerabilities coming from cyberspace than its national cybersecurity strategy does. The national security document states that critical infrastructure as a whole is exposed to a number of threats with natural, technological, and asymmetric aspects. Examples of such threats include cyberattacks, economic crime, and sabotage among others (Cyber Security Strategy of the Czech Republic for years 2011–2015, 2011). In other words, countries which are keen on securitizing their cyberspace are more likely to prioritize the safety of critical infrastructure as a key condition of national security. Because national security is linked to critical

infrastructure as the referent object, the actors with power to identify objects that require security and defense may claim the right to use extraordinary means in the name of security. For example, Poland's cybersecurity doctrine emphasizes the importance of critical infrastructure and a direct relationship between cybersecurity and the country's proper functioning, including its economic development and the ability to operate effectively in the military sphere (Cybersecurity Doctrine of the Republic of Poland, 2015). What is more, Poland is the only country which is willing to develop not only defensive but also offensive cyber capabilities in order to deter potential opponents in cyberspace (National Security Strategy of the Republic of Poland, 2012). Thus, Poland's approach reveals that the more articulated the process of identifying and defending against cyber threats is, the more militarized it becomes.

On the other hand, countries such as Hungary and Slovakia also mention critical digital infrastructure as a referent object. However, these countries do not view potential attacks on critical infrastructure as a threat to national survival, as cybersecurity in these two countries is thought to be just one of several national security sectors. Hungary and Slovakia focus mainly on information security. The objectives of Slovakia's information security strategy focus on protecting human rights and freedom, improving information security management, and defending state ICT in order to support the state's critical infrastructure (National Strategy for Information Security in the Slovak Republic, 2008). The concept of referent objects in Hungary's cybersecurity strategy remains even more ambivalent; it lacks any direct reference to primary referent objects. The strategy only mentions protecting national data assets and the "operational safety of the parts of its critical infrastructures linked to cyberspace" (Government Decision on the National Cyber Security Strategy of Hungary, 2013). Neither Slovakia nor Hungary identifies a specific referent object that should be protected first within cybersecurity; as a consequence both countries have a decidedly civil approach to cybersecurity.

Perceptions of Cyber Threats

The securitization of cyber issues is based on different discourses, most commonly in national security discourse. Therefore, cyber issues usually arise when agents, such as foreign governments or non-state actors, with rogue intentions attempt to gain access to financial, energy, or public-safety systems, and the prospect of cyberattacks is presented as a threat that requires an urgent response. Perceiving and presenting cyberattacks in this manner lead to intense security measures. Consequently, in countries where a national security discourse prevails, the threat of cyberattacks are regarded as a top priority, and there is a military approach to cybersecurity.

However, threats to cyber- and national security do not arise from external sources alone. Hence, cyberattacks can also arise from systematic threats. These systemic threats, defined by Hundley as "cyberspace safety," stem from the inherent unpredictability of computers and information systems, which "create unintended

(potentially or actually) dangerous situations for themselves or for the physical and human environments in which they are embedded" (Anderson and Hearn 1996). A more common issue, however, is intentionally provoked systematic threat invoked by criminal syndicates or individuals. In this regard, technical discourse is accompanied with a criminal one and is linked to cybersecurity discourse. In this discourse, cybersecurity can, in short, be seen as safeguarding computers from criminal activity, and cyberattacks are perceived not as national security threats but as common risks in the cyber sector. Consequently, countries that perceive potential cyberattacks as a risk for a particular sector are less keen to define cyber issues as issues of national security and can be identified as civil-oriented states.

Poland, Latvia, Lithuania, Estonia, and the Czech Republic have a multilayered approach to cyberattacks. First, they evaluate risks to their national security and task state institutions with preventing cyberattacks. Secondly, they identify cyber-related challenges to the integral components of their national security: the economic, financial, and private sectors. This comprehensive approach to cyberattacks is reflected in Estonia's cybersecurity strategy. Estonia claims that it has a growing number of state actors tasked with countering cyber espionage and protecting both Internet-connected and closed networks, with the additional aim of collecting information on security and economic interests (Cyber Security Strategy of Estonia 2014–2017, 2014). National security is also the prevailing discourse in Poland's cybersecurity doctrine. The cyber threats identified in Poland's doctrine include attacks against telecommunications systems important to national security and cybercrime – specific cybercrimes mentioned in the doctrine include "cyber violence, destructive cyber protests and cyber demonstrations," data and identity theft, and private computer hijacks (Cybersecurity Doctrine of the Republic of Poland, 2015). The same discourse is seen in Lithuania and Latvia's strategic documents. For example, Lithuania's state defense concept groups cyberattacks as a national threat together with terrorism and organized criminal activities (the State Defense Concept of the Republic of Latvia, 2012). It is worth mentioning that Latvia's newest national security concept highlights cyberattacks as one of eight primary national security threats (Press release, 2015).

The four countries mentioned above have a comprehensive approach to cybersecurity based on precise evaluations of the potential impact of cyberattacks on different sectors and on national security overall. Since the cyberattacks are perceived mainly as threats to national security, these countries have responded with a military approach.

Slovakia's updated cybersecurity concept for 2015–2020 also presents a complex perception of cybersecurity. Slovakia claims that cybersecurity should not be seen as an isolated problem of the Slovak Republic or as an issue isolated to one or even several sectors and that, due to its global nature, cybersecurity is a society-wide phenomenon (Cyber Security Concept of Slovak Republic for 2015–2020, 2015). The document also identifies the core problem of Slovakia's cybersecurity policy: that cyber threats are not generally seen as a sufficiently urgent problem and are not explicitly or validly addressed in Slovak law (Cyber Security Concept of Slovak Republic for 2015–2020, 2015). While this document is instrumental in its nature, as it offers a model for managing cybersecurity policies, it lacks a complete

vision of cybersecurity challenges. As a result, potential cyberattacks are seen mainly as risks to unnamed targets.

The strategy of the Czech Republic mentions risks such as cyber espionage (industrial, military, political, or other), organized crime in cyberspace, hacktivism, intentional disinformation campaigns with political or military objectives, and even – in the future – cyber terrorism (Cyber Security Strategy of the Czech Republic for the 2011–2015 period, 2011). These risks are seen mainly as dangerous tendencies in the global cyberspace that have not yet threatened Czech society. The security discourse that prevails in the strategic documents of the Czech Republic mainly refers to systematic threats and "computer safety." In this regard, the Czech Republic's cybersecurity strategy focuses mainly on building a credible information society by safeguarding access to services, protecting data integrity, and promoting the confidentiality of the Czech Republic's cyberspaces (Cyber Security Strategy of the Czech Republic for the 2011–2015 period, 2011). Meanwhile, Hungary also emphasizes the criminal element of cyberattacks. Thus, Hungary claims that dynamically developing new technologies, like cloud computing and mobile internet, leads to the continuous emergence of new security risks, such as illegal acquisitions of critical information and personal data (Government Decision on National Cyber Security Strategy of Hungary, 2013). Moreover, Hungary avoids identifying cybersecurity challenges with threats. It prefers to name cyber threats as risks to the cyber sector.

The perceptions of cyber threats and cybersecurity in general determine the civil approach to cybersecurity management that prevails in the Czech Republic, Slovakia, and Hungary.

Sources of Cyber Threats

The cyberspace's architecture facilitates anonymity and hinders attempts to track the sources of cyberattacks, constituting an additional factor of insecurity. Nevertheless, it is possible to analyze the sources of cyberattacks and cyberattackers, who may operate as functional actors. The logic of such analysis would be similar to what representatives of the Copenhagen school sketch out in analyzing the pollution of the environment: these actors directly influence the dynamic of the cyber sector, but they are neither referent objects nor securitizing actors, though they may contribute to actions that impact the perception of the threat (Buzan et al. 1998). In a civil-military dichotomy, external cyber threats such as foreign states or non-state actors, including cyber terrorists and cyber espionage agents, clash with internal actors: hacktivists, cybercriminals, malware authors, cyber scammers, and corporations. As mentioned previously, countries that are actively securing their cyberspaces emphasize the political motivation of cyberattacks and external cyber threats. This attitude dictates a military approach to cybersecurity management as the most effective. Conversely, focusing mainly on internal cybersecurity threats means that the main referent object is the economic sector or private data. To fight these threats, a civil approach to cybersecurity policy is thought to be sufficient.

Further analysis of how the sources of cyber threats are understood by particular countries brings us to the conclusion that all countries acknowledge that there are many actors in cyberspace; however, only a few states make a distinction between nature, objectives, and methods of these actors. For example, Estonia's cybersecurity strategy claims that national cybersecurity is affected by the actors operating in cyberspace with various skills, targets, and motivations and that cyber espionage – with the intent to collect national security and economic information – is increasing. Estonia's strategy also emphasizes that the number of states capable of and actually initiating cyberattacks is increasing (Cyber Security Strategy of Estonia 2014–2017, 2014). This distinction between internal and external threats is also made in the Polish doctrine. External threats listed by the doctrine include cyber crises, cyber conflicts, cyberwar, and cyber espionage involving states and other entities, "threats (for Poland) coming from cyberspace include extremist, terrorist and international criminal organizations whose attacks in cyberspace can have ideological, political, religious, business or criminal motivations" (Cyber security doctrine of the Republic of Poland, 2015).

Lithuania and Latvia, in contrast, haven't identified specific cyberattackers, but their strategic documents refer primarily to external threats, such as neighboring countries. Meanwhile, both Slovakia and Hungary have quite a blurred and fragmental vision on the sources of cyber threats. For example, Hungary focuses on technological (internal) vulnerabilities and their effects to the proper functioning of the state's economy without any deeper analysis of their causes and actors engaged into the process. The cybersecurity strategy of Hungary states that in addition to the damage caused by external factors, the inadequate regulation of the operational security of the information and communication systems constituting cyberspace poses a further risk. "Dynamic emerging new technologies, such as cloud computing or mobile Internet, lead to the continuous evolution of new security risks" (Government Decision on National Cyber Security Strategy of Hungary, 2013). The civil approach to the sources of cyber threats is also common to the Czech Republic. The National Security Strategy of the Czech Republic identifies a wide range of potential cyber challenges; however, almost all of them are criminal or technological in nature. These are hackers stealing personal or sensitive data, technological failures, botnets, DDoS/DoS attacks, etc.

The perception of cyber threats is closely linked to the sources of the perceived threats. The more securitized a view of cyber threat prevails, the more precisely the source of a threat is identified. What is more, countries that securitize cyber threats, such as Estonia, Poland, Lithuania, and Latvia, make a distinction between external and internal cyberspace actors. Meanwhile, countries that emphasize the criminal element of cyber threats think about them as internal challenges and limitations of cyberspace. It is noteworthy that almost all of the analyzed countries make a distinction between internal and external sources of cyber threats in their strategic documents. However, the countries that are described as civil-oriented are not keen on elaborating this distinction further and focus mainly on internal threat sources as the most common and probable in their security environment.

Conclusion

The qualitative analysis of the cybersecurity policies of the four Visegrad countries and the three Baltic States shows that each of these countries has cybersecurity strategies and corresponding laws to address cybersecurity issues. All of the documents analyzed refer to higher-level national security or defense strategies and present the legislative environment, although there are significant differences in their profundity. Different cyberspace entities and the potential threats these entities generate are also addressed in the documents. In most national cyberspace security strategies, threats to critical infrastructure and cybercrime play a prominent role and indicate increasing economic damage wrought by cyberattacks. In the formal sense, the domain of cyberspace is already included in the security agendas of all states and could be called "securitized."

However, there are differences of securitization among countries. Cybersecurity differs by how countries (1) define a referent object (what should be protected), (2) perceive primary threats and risks, and (3) identify the sources of threats and risks. In accordance with these differences, countries can be classified into two categories. The first category, that of countries that militarize cybersecurity issues, includes Poland, Estonia, Lithuania, and, to some degree, Latvia. These countries that have militarized cybersecurity discourse are more precise in identifying specific referent objects and in articulating the defense of these objects as national priorities. This tendency elevates cybersecurity to the highest national security level and focuses on safeguarding ICT and governmental information resources. Poland, Estonia, and Lithuania tend to identify cybersecurity challenges as threats to the proper functioning of the state and identify attacks from foreign states as the most dangerous sources of such threats. Consequently, in these states, the responsibility of responding to cyber threats is handed over to military and defense institutions.

The second category of securitization discourse refers to the criminalization of cybersecurity issues. The Czech Republic, Slovakia, and Hungary rely on a civil approach to maintain cybersecurity. Their referent objects are diffused and mainly related to the proper functioning of the state's economic system and private property. The ICT and governmental digital resources have no priority over other legitimate referent objects. As a result, countries with a prevailing civil approach are mostly concerned with criminal activity conducted in cyberspace and describe cybersecurity issues as "risks." Potential sources of such risks are also fragmented and include not only external international actors but also internal actors such as hackers, hacktivists, criminal organizations, and even the unintentional disruption of networks. Civil institutions in the Czech Republic, Slovakia, and Hungary are charged with monitoring cybersecurity risks and coordinating state response to cyber incidents (Table 2).

The conclusions of this chapter, the categorization of cybersecurity approaches as civil or militarized may lead to a better understanding of cybersecurity as a phenomenon. It could contribute to the explanation of obstacles for cooperation between states dealing with cybersecurity issues on the international level. Furthermore, the identification of different approaches to cybersecurity could explain specific state's actions in cyberspace. Understanding states' differences in perceiving cyber threats,

referent objects, and potential adversaries constitutes a background to discussions of the so-called cyber identities of states and nongovernmental actors. This could be a useful theoretical tool for analyzing potential cyber conflicts and cooperation patterns in further studies.

References

Anderson, R. H., & Anthony, H. (1996). An exploration of cyberspace security R&D investment strategies for DARPA: "The day after. . . in cyberspace II".

Butrimas, V. (2015). National security and international policy challenges in a post Stuxnet world. *Lithuanian Annual Strategic Review*. Lithuania: Ministry of Internal Affairs.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder: Lynne Rienner.

Deibert, R. J. (2002). Dark guests and great firewalls: The Internet and Chinese security policy. *Journal of Social Issues, 58*, 143–159. https://doi.org/10.1111/1540-4560.00253.

Deibert, R., & Crete-Nishihata, M. (2011). Blurred boundaries: Probing the ethics of cyberspace research. *Review of Policy Research, 28*, 531–537. https://doi.org/10.1111/j.1541-1338.2011.00521.x.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review.* https://doi.org/10.1111/misr.12023.

European Union Agency for Network and Information Security (ENISA). (2012). Cyber Europe 2012, key findings report, European Union Agency for Network and Information Security.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security and the Copenhagen School (2009). *International Studies Quarterly, 53*, 1155–1175. Available at SSRN: https://ssrn.com/abstract=2567410.

Harknett, R., & Stever, J. A. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management*. Berlin/New York: De Gruyter.

Lobato, C. L., & Kenkel K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional*, *58*(2), 23–43. Available at http://www.scielo.br/pdf/rbpi/v58n2/0034-7329-rbpi-58-02-00023.pdf.

Moore, T. (2010). *Introducing the economics of cybersecurity: Principles and policy options*. National Academies of Sciences Engineering Medicine (NAP).

Newmeyer, K. P. (2015). Elements of national cybersecurity strategy for developing nations. *National Cybersecurity Institute Journal, 1*(3), 9–19. Excelsior College, Albany.

Saco, D. (1999). Colonizing cyberspace: "National security" and the Internet. In J. Weldes, M. Laffey, H. Gusterson, & R. Duvall (Eds.), *Cultures of insecurity: States, communities, and the production of danger*. Minneapolis: University of Minnesota Press.

Šaljić, E., & Đorđević, Z. (2011). Modern forms of terroism [!] environmental terrorism. Retrieved from https://dk.um.si/IzpisGradiva.php?lang=eng&id=30223.

Świątkowska, J., et al. (2012). *V4 cooperation in ensuring cyber security – Analysis and recommendations*. Krákow: Koscluszko Institute.

UNIDIR. (2013). *The cyber index. International security trends and realities*. Geneva: UNIDIR, United Nations Institute for DIsarmament Research.

Annotated Bibliography on the Impact of Geofencing as a Security Strategy Model

49

Anthony Chukwuemeka Ijeh

Contents

Abstract

Aim: This article looks at the societal impact of a research study 10 years after it obtained proof of concept as a prototype for surveillance. The solution was used to continuously monitor communication of a mobile device and intercommunication unit within a defined space. **Introduction**: Citations of a key reference article written on the use of Geofencing as a Security Strategy Model were retrieved and reviewed to assess its real-world use and societal penetration. **Motivation**: After nearly

A. C. Ijeh (✉)
College of Computer Information Technology, American University in the Emirates, Dubai, UAE
e-mail: anthony.ijeh@ieee.org

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6_63

10 years of publishing the first paper on Geofencing as a Security Strategy Model and launching the prototype for commercial purposes, this paper's motive is to evaluate its societal impact. **Problem statement**: The impact of applied technological research can be obvious, but the benefits of basic research which this was as at the time can be difficult to assess. **Approach**: To standardize the collection of information related to the reference work, the review used keyword searches of academic repositories and electronic databases from September 2009 to February 2018, including Google Scholar. The survey was done in batches to enable ease of flow and analysis. **Result**: The model's transferability and application have no limitations as the concept and its implementation are simple and draw on existing technologies which are available and at low cost. **Conclusion**: Key citations of a paper which uses surveillance technology written in 2009 have been gathered to ascertain past and future trends of its uses within academia and in practice.

Keywords
Annotated · Bibliography · Bibliometric · Survey · Geofencing · Surveillance · Technology · Security · Strategy · Model · Research · Assessment · Impact · Prototype · Tracking · Citations

Introduction

This annotated bibliography presents citations of resources which refer to Geofencing as a security strategy model (Ijeh 2010a). Several examples of its practical use are used to demonstrate its functionality and applicability in the joint realm of location-based services and wireless networks. In wireless communication which uses air as a medium, electromagnetic radiation permeates through walls, closed doors and windows of building structures allowing signals to be intercepted by unauthorized users using specially equipped laptops outside the buildings controlled by physical space Ijeh et al. (2009). The approach creates a virtual perimeter around the defined space. After several experiments in different UKAS-accredited laboratories under different conditions, readings showed that communication between a mobile device and intercommunication unit could be monitored within defined space. This bibliography lists recent and historical works which cite the published doctoral thesis titled Geofencing as a Security Strategy Model (Ijeh 2011). The citations are from a variety of published formats and include serials, articles, websites, monographs (which include manuals, dictionaries, and handbooks), conference and workshop proceedings, and patents.

Research Impact

Research Councils UK (RCUK) defines research impact as "the demonstrable contribution that excellent research makes to society and the economy." This can involve academic impact, economic and societal impact, or both: Academic impact

Table 1 Bibliometric indicators used in this study

Sources	Year range	Downloads	Process	Citations	Leads
48	2009–2016	Unknown	Peer reviewed	48	Unknown

shifts the mind-set of individuals and advances science, theory, and application across disciplines. Economic and societal impact benefits individuals, organizations, and/or nations. This paper surveys the demonstrable contribution of the concept and prototype as an intervention used by people in their daily lives, organizations in their supply chains, and countries for their political, economic, social, or technological development.

Research Approach

The review involved keyword searches of electronic databases from September 2009 to February 2018, including Google Scholar. The following search terms were included: "Geofencing" *and* "as" *and* "a" *and* "security" *and* "strategy" *and* "model." The review included serials, articles, websites, monograph, books, patents, thesis, newspapers, magazines, conference and symposium proceedings, and conceptual models for assessing research impact. The review was conducted from February 2016 to February 2018 using full papers citing the reference work and using the following criteria: (i) articles used were published in English between 2010 and 2018, (ii) used articles referenced or described the source papers intervention, and (iii) articles were demonstrations of how Geofencing as a Security Strategy Model had been applied in different context.

The strengths and weaknesses of bibliometric methods are discussed to assess the usefulness of this paper and its impact on society. Bibliometric assessment is usually based on one central assumption which is that scientists are expected to publish their research in peer-reviewed journals (Van Raan 2003). Bibliometric indicators used include sources, year range, downloads, process of review, number of citation, and leads (author/institution) as shown in Table 1 and Fig. 1.

Serials

The serials used contain some of the most recent and varied information on off-spring topics from Geofencing as a Security Strategy Model. Topical information often appears in serials well before monographs. DOI, current publisher, previous title, frequency, serial type, and beginning year of publication were verified through Ulrich's Periodicals Directory. Published since 2013, this quarterly serial offers general information and news about health and healthcare in the Internet age. The study in question looks at the increasing elderly population and the need to provide care and safety at a high level with limited resources. It proposes that a new social alarm solution may contribute to safety and independence for many elderly. The

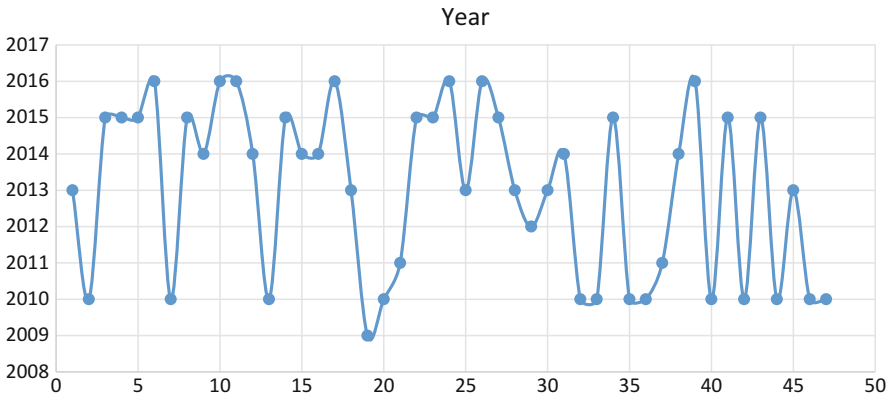


Fig. 1 Year range and citations

work studied social alarms in a broad sense and from several user perspectives. In the first study, social alarm use and its aspects were investigated. To understand where there may be problems and weaknesses, users, caregivers, managers of municipalities, and personnel at alarm centers were interviewed. The studies' interviews helped identify a number of problems. For municipalities, the processes of procuring new alarms and managing their organization were found to be complex. The effect of this was that the same social alarm systems had been ordered over and over again without taking into account new user needs or new technical solutions. For alarm users, one large problem was that the alarms had very limited reach and were designed for indoor use only. This has resulted in users hesitating to leave their homes, which in turn has negative effects due to lack of physical activity and fewer social contacts. One important result from the first study was the need for a social alarm solution that worked outdoors. In a second study, needs regarding outdoor social alarms were investigated. The results from this study showed that wearable outdoor alarms must be easy to use, provide communication, and be well designed. In addition, the alarms must work both indoors and outdoors, and the user should not have to worry about where he/she is or who is acting on an alarm (Marie 2014).

Articles

This section contains information on articles from a variety of serials (not limited to the titles from the previous section). While most of the articles are from the past few years, an example of an article discussing Geofencing as a Tool for Participatory Processes by the UN-Habitat is included to indicate that the topic has been adopted and recognized by the United Nations as a major tool for circumvention of some of today's problems. Published by the UN-Habitat, the article puts forward a conceptual framework to improve citizen engagement and participation in public consultation processes through the application of location-based services (Geofencing). The

conceptual framework aims to strengthen the capacity of developing countries in applying technologies that can capture, store and process, communicate, and display opinions from citizen engagement during public consultation. The purpose of the article is to present the conceptual framework which offers a perspective of Geofencing in public consultation that improves access to information as well as promotes participation in policy-making for the empowerment of the individual citizen and for the benefit of society as a whole. The article considers existing technologies and models used in the design and development of electronic governance. In addition, the article considers and defines the issues with the use of existing technologies and models for electronic participation. The article recommends the framework as circumvention to existing barriers to effective citizen engagement which cause low electronic participation during public consultation (Ijeh 2015).

The journal article discusses real-time location tracking and monitoring of physical objects that require physical access within a specified geographical area. It talks about unauthorized access being restricted within the same area for purposes of security and refers to Geofencing as a key tool for real-time location tracking which is implemented by GPS or beacons or RFID (Dabhi 2016).

The journal article reports on how location-based services are routinely used and gives examples of how their use provides a user's location to the public when in use. The article discusses the need for privacy enhancement in location-based services using Geofencing as other methods have deficiencies which can be overcome or decrease the quality of service. It highlights the strengths of Geofencing and why its use secures access to only authorized persons. It then looks at the components and model being used to design and develop Geofencing (Jaltare and Holey 2016).

In this research project, an article is used to discuss Geofencing as a virtual parameter with an adjustable radius to suit the different geographical needs of users. The article informs that Geofencing has widely increasing scope including proactively informing the user about location-specific information (Rahate and Shaikh 2016).

The article discusses the problems with small unmanned aircraft systems (UAS) and how Geofencing can be used to ensure safety. It talks about challenges caused by identification of hazard source potentials to UAS when they are operational. The article reports that Geofencing can be used to identify objects within a geographical area. UAS hazard identification could be formally modelled on the Geofencing concept to enhance safety and airworthiness standards (Luxhoj 2016).

A research team investigated a challenge caused by the popularity of unmanned aircraft systems (UAS) that gives rise to a risk of collusion between commercial aircraft and UAS near airports. The article proposes a module called the Airport Secure Perimeter Control System to mitigate the risk of collusion. The module uses a database containing central coordinates of all airports in the USA to prevent UAS from entering a 5-mile radius of airports. Once the radius is breached, autopilot takes over control of the UAS and lands it in a controlled manner (Boselli et al. 2016).

The authors describe a new way of providing security for objects like cars or files using Geofencing. The article describes the functionality of the model which notifies the user when an object moves out of the fence. Encryption is used to provide

security and the paper explains how a key generation for decrypting files at the same location and by the same person where it was encrypted and decrypted happens. The research study also discusses security for cars and how the engine locks when the fence is exited and the vehicle is used by an unauthorized person (Prabu et al. 2011).

The article describes the increase in usage of mobile devices such as smartphones and tablets over the years. The article presents statistics which shows that individuals own more than one phone, and this has caused the problem of nuisance ringtones to double. The study reports that Geofencing can be used to block phones from ringing in quiet areas and spaces such as meetings, classrooms, libraries, auditoriums, etc. (Zin et al. 2016).

The journal article contributes to knowledge on deploying cloud computing in an enterprise infrastructure which brings significant security concerns. The journal discusses security and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. The journal also discusses the importance of security in mobile technology using infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Here all kinds of authentication mechanisms are used such as SAML-based, SSO, and LDAP-based authentication for more security. For authorization XACML is used. The journal reports that by following OSGi, standard security plug-in has been developed so that anybody can just add the plug-in as a JAR file and get the security features such as LADP registration and authentication. The journal concludes that its proposed solution is more flexible and compact than others (Akshay and Apoorva 2014).

The journal describes how social media increases in functionality and popularity, making it more vulnerable. It reports that social media vendors exclude security during development, hence leaving it to users' discretion which raises a serious cause for concern. The aim of the research undertaken is to study existing vulnerabilities of online social media and propose practical solutions. The importance of studying social media vulnerabilities provides a clear understanding in developing a new security model to prevent social engineering attacks. The journal investigates key security vulnerabilities eroding the trust placed on social media such as profile cloning, single-factor authentication, weak password creation, weak account activation systems, privacy vulnerabilities, unethical posts, and multiple log-in sessions. The journal concludes by proposing its solution as a novel social media security model (SMSM) to reduce the aforementioned vulnerabilities (Ikhalia 2013).

This article is published by the Electronic Frontier Foundation (EFF), a member-supported, nonprofit public interest organization devoted to maintaining the traditional balance that copyright law strikes between the interests of rights holders and the interests of the public. Founded in 1990, EFF represents over 25,000 dues-paying members, including consumers, hobbyists, artists, writers, computer programmers, entrepreneurs, students, teachers, and researchers, who are united in their reliance on a balanced copyright system that ensures adequate incentives for creative work while promoting innovation, freedom of speech, and broad access to information in the digital age. In filing these reply comments, EFF represents the interests of the many people in the USA who have "jailbroken" their

cellular phone handsets and other mobile computing devices – or would like to do so – in order to use lawfully obtained software of their own choosing and to remove software from the devices (Federal Register 2015).

The article explains Geofencing and how it works and its applications in the real world, including how they pertain to information security, and also elaborates the strengths, weaknesses, opportunities, and threats associated. The author includes more information about implementing a Geofence within a wireless network and the methodology used to contain, fingerprint, and allow mobility of secure data across a network. Geofencing is shaping our world, and information security professionals need to develop strategies for it in regard to information assurance (Haddock 2016).

The article is an output from a project sponsored by the company known as AT&T which has a need for a device that has the capability to communicate with other devices in meaningful ways. In a world where humans are becoming more and more connected through wireless devices, there is always room for a new product that can make life easier. The goal and purpose of this project are to design a wearable device that has many features that makes everyday life more convenient via wireless transfer. A key point in the design is to limit human interaction. The device will be programmed by the user to perform tasks automatically. The product will be lightweight, comfortable, and esthetically pleasing. In developing the design, several different concepts were considered. Some of the biggest questions asked were: Which type of wearable device would be the most comfortable and which type would be the most efficient and effective (Marchetti 2014)?

After reviewing these questions, it was determined that a bracelet would be the best option. The bracelet would be able to communicate with other devices around the home such as wall outlets and electronic locks in order to perform tasks. Tasks include unlocking the front door (hands-free) and turning on lights, fans, etc. A few problems arose such as how the device would effectively track the user's location indoors. These problems were dealt with, and the resulting product does its job effectively. Several limitations are presented with this prototype design. The article postulates that the final product must have a large enough battery to be sustainable for a long period of time. It must be able to operate in adverse weather conditions. The product must also be compact and comfortable for the user to wear. The product must also be affordable, so keeping under budget and on schedule are both significant limitations. These limitations were faced, and the final product met all necessary requirements (Marchetti 2014).

Websites

Websites provide valuable and up-to-date information on a variety of monographs and are able to go into extensive detail on topics concerning Geofencing as a Security Strategy Model. The monographs covered in this section cover a variety of topics on Geofencing as a Security Strategy Model. Some address wireless security as a whole, while some focus on a specific Geofencing aspect. Some items target those working in the area of information security, while others are

written with general readers in mind. While the majority of the monographs are published in the past 5 years, a few examples of earlier works are included. Since many websites are timely and require the need for information to be readily available, websites are valuable resources. The sites are managed by a variety of organizations, including societies, government agencies, businesses, educational institutions, and nonprofit agencies. Published by pdvWireless, the article looks at mapping technology which has experienced some of the most rapid involvements within the emerging technology era. The widespread adaptation and utilization of global position system (GPS) technology have paved the way for many technologies to be built surrounding location data. The article reports Geofencing tools as a significant element within this space, which has revolutionized the way that we view, understand, and segment location data across a variety of businesses.

However, Geofencing faced much scepticism in its earlier age. Prior to the technology developments that we have seen firsthand across a variety of industries, the technology development process behind Geofencing was deemed as very cumbersome and costly to deploy. Recently, it has evolved into a complex and revolutionary location-centric application, serving a plethora of business sectors. The amalgamation of real-time data, and geographic information, allows businesses to gain insight from data that can be used toward company strategy and decision-making. The Geofencing technology market as a whole is projected to reach 300 million dollars by 2017 (Grosinger and Hackett 2014).

Published by the HIPAA Journal, the article looks at improving healthcare data security and asks if Geofencing is the answer. Geofencing is a technique that can be used to improve healthcare data security by limiting the information that individuals can access on devices and also the physical locations where access is permitted. A Geofence is a virtual perimeter that can be applied to software which corresponds to a geographical boundary in the real world. It is possible to set virtual boundaries by using global position satellite (GPS) signals or radio-frequency identification (RFID). In a healthcare environment, Geofencing could allow IT professionals to exercise greater control over PHI and where it can be accessed. For example, a laptop computer that is used in a hospital can have a Geofence installed which will only allow PHI to be accessed within the boundaries of the building. If that laptop is taken out of the hospital, administrators will be able to remotely – and automatically – prevent hospital systems from being accessed. It is also possible to set up multiple Geofences to allow devices to be used in any hospital run by a healthcare provider or even to include physicians' homes within the fences. In addition to limiting the physical locations where data can be accessed, it is also possible to use the technique to track employee devices, restrict the applications that can be used and the websites that can be visited, or for access to be restricted to specific working hours.

According to Roman Foeck, the founder and CEO of CoSoSys – a company that employs Geofencing – the system is not infallible as it is possible to fool the GPS and therefore get around the perimeters applied by healthcare IT professionals. In the case of CoSoSys, this issue was tackled by the use of other beacons in addition to a GPS signal, such as Wi-Fi or Bluetooth. Foeck says, "If you rely on a second factor –

like proximity to some other devices, such as secure beacons that act as tokens – that cannot be spoofed," provided the privacy and security concerns are addressed and Geofencing can be made secure – and infallible – the benefit to the healthcare industry could be considerable. Geofencing could potentially prevent many HIPAA breaches from occurring, especially in the case of lost or stolen mobile healthcare devices (HIPAA 2015).

Monograph

Monographs are able to go into extensive detail on Geofencing as a security strategy model application. Some address Geofencing as a whole, while some focus on a specific aspect. Some items target those working in the area of Geofencing security, while others are written with another field with the general reader in mind. While the majority of the monographs are published in the past 5 years, a few examples of earlier works are included. The article presents several new query processing techniques, called complex motion pattern queries, specifically designed for very large spatiotemporal databases of moving objects. The brief begins with the definition of flexible pattern queries, which are powerful because of the integration of variables and motion patterns. This is followed by a summary of the expressive power of patterns and flexibility of pattern queries. The brief then presents the Spatiotemporal Pattern System (STPS) and density-based pattern queries. STPS databases contain millions of records with information about mobile phone calls and are designed around cellular towers and places of interest. Density-based pattern queries capture the aggregate behavior of trajectories as groups. Several evaluation algorithms are presented for finding groups of trajectories that move together in space and time, i.e., within a predefined distance to each other. Finally, the brief describes a generic framework, called DivDB, for diversifying query results. Two new evaluation methods, as well as several existing ones, are described and tested in the proposed DivDB framework. The efficiency and effectiveness of all the proposed complex motion pattern queries are demonstrated through an extensive experimental evaluation using real and synthetic spatiotemporal databases. This clear evaluation of new query processing techniques makes spatiotemporal database a valuable resource for professionals and researchers studying databases, data mining, and pattern recognition (Veira and Tsotras 2013).

The article looks at recent trends and reports that there is a big percentage of the population, especially young users, which are smartphone users and there is a lot of information to be provided within the applications; information provision should be done carefully and should be accurate, otherwise an overload of information will be produced, and the user will discard the application which is providing the information. Mobile devices are becoming smarter and provide many ways to filter information. However, there are alternatives to improve information provision from the side of the application. Some examples are, taking into account the local time, considering the battery level before doing an action and checking the user location to send personalized information attached to that location. Smart campus and smart

cities are becoming a reality, and they have more and more data integrated every day. With all this amount of data, it is crucial to decide when and where the user is going to receive a notification with new information. Geofencing is a technique which allows applications to deliver information in a more useful way, in the right time and in the right place. It consists of Geofences, physical regions delimited by boundaries, and devices that are eligible to receive the information assigned to the Geofence. When devices cross one of these Geofences, an alert is pushed to the mobile device with the information (Muriach 2015).

Books

This new resource presents the principles and applications in the emerging discipline of *Activity-Based Intelligence* (ABI). This book will define, clarify, and demystify the trade craft of ABI by providing concise definitions, clear examples, and thoughtful discussion. Concepts, methods, technologies, and applications of ABI have been developed by and for the intelligence community, and in this book, you will gain an understanding of ABI principles and be able to apply them to activity-based intelligence analysis. The book is intended for intelligence professionals, researchers, intelligence studies, policy-makers, government staff, and industry representatives. This book will help practicing professionals understand ABI and how it can be applied to real-world problems (Biltgen 2016).

Patents

Published by the Intellectual Property Office UK, this patent of Geofencing as a Security Strategy Model presents an invention for wireless network availability based on the location of a mobile device. When using a wireless network to operate a mobile device, e.g., a laptop, Wi-Fi Protected Access 2 (WPA2) is often used to camouflage the data being sent and received from appearing as clear text. However the challenge in using just WPA2 is that it does not prevent code-breaking war drivers from obtaining wireless networks available within the area or code breaking the encryption to view data as clear text. To overcome these problems, this patent presents a wireless security model for securing wireless network availability against war-driving code breakers. The wireless security model is made up of a security solution and security strategy. The evaluation of the wireless security model is undertaken using a test bed with 802.11 legacy-mode network availability. The demonstration results show that the invention is able to successfully make the wireless network unavailable to war drivers and that security policies can be used to control network availability within the test bed parameters. The patent submission article is sectioned as follows: Introduction, Existing Literature, Component Specification, Demonstration, and Claim (Ijeh 2010a).

This patent is for architecture that enables Geofence combinations and compositions where multiple correlated Geofences are generated for an entity such as a point

of interest. The Geofences can have varying radii relative to a specific entity and represent distinct areas or aspects of the entity. The Geofences can relate to correspondingly different categories to which the entity can belong. The Geofences can be of differing shapes than circular, such as polygons (e.g., rectangles, squares, etc.). Moreover, these differently shaped Geofences can be applied to a single entity. Each Geofence of a set associated with an entity can be assigned to represent different parts of an entity such as a part of a shopping mall. Geofence composition is obtained by combining multiple primitive Geofences to compose more complex Geofence (s) for an entity and for embedding the relationship of the primitive Geofences into such compositions (Parab et al. 2013).

A patent for disclosed embodiments is presented and discussed, it relates to a wireless human machine interface ("HMI") for a programmable logic controller ("PLC") implemented in a mobile device which selectively enables an operator's access and control of the PLC's functionality. The PLC's functionality is based on the location of the mobile device, allowing various subsets of operations to be performed from suitable locations. An efficient operation of the PLC 102 is achieved while complying with requirements for adequate protection of personal safety and protection of property (Long 2013).

Authors of this patent claim it is for one embodiment of an electronic device comprising a display, a motion sensor, one or more wireless communication devices, and logic configured to receive via the controller, data indicating that the controller is in motion. It also determines the velocity of the controller and activates its first location service to determine coarse location of the controller when velocity falls below a predetermined threshold for a predetermined period of time (Modali et al. 2014).

Claims made in this patent are for a branch device of Geofencing pairing security which provides security for a sensitive item using distance as a parameter. Two trackable devices are used to track each other within a dynamic perimeter, and both are informed when the other leaves the dynamic perimeter (Fernandez and Birse 2014).

Thesis

Published by the highly esteemed Naval Postgraduate School, the thesis addresses the threat to public safety by vehicles being used by criminals or terrorists to commit violent acts. The impact of the article on international law enforcement standards is high because vehicles are being used as the new tool for committing acts of extreme violence by terrorists. The article identifies the vulnerability of vehicles as non-availability of three core measures: theft prevention, authorized use, and ability to track and recover vehicles that get into the wrong hands. A model is presented for law enforcement agencies to secure vehicles using SERVE technology which has four tiers. Tier I covers theft prevention, Tier II covers authorized use, Tier III covers tracking and recovery, and Tier IV covers human-machine interface (Johansmeyer 2013).

Magazines and Newspapers

The magazine article reports that Geofencing can restrict access to devices or applications while inside a company's perimeter, making it impossible for devices outside the perimeter to access the network, explains Roman Foeckl. As data breaches continue to grow in complexity, severity, and frequency and organizations face growing threats – internal and external and deliberate and unintentional – new and more advanced technologies are needed to keep critical information safe. As demonstrated by the Anthem Insurance breach in the USA, when sensitive information gets in the wrong hands, it can be incredibly costly – experts are estimating that it could cost the company upward of 100 million dollars (66 million pounds sterling) in this case (Foeckl 2015).

In this magazine article, a senior official was asked about the legality and mechanism of getting Geofencing facility from the mobile phone companies after it was denied to the police by the interior ministry; he said it was just "an understanding" between the law enforcement agency and mobile phone companies "for the time being." "Geo-fencing in a security strategy model, provides security to wireless local area networks," said the official. "It's a modern technology being used by the investigators across the world and that could only be done through cellular companies' assistance. We only engage cellular companies in high-profile cases. Interior ministry has not yet allowed it but the police are now going to implement it through understanding with the companies. As far as a formal nod is concerned, we are also in touch with the interior ministry to resolve the issue for once and all" (Ayub 2015a).

The author of this magazine article said access to subscribers' data Geofencing, officially, remained an exclusive privilege of the spy agencies, while the police could not get a nod from the interior ministry or assistance from the powerful intelligence apparatus for that purpose. "Geo-fencing in a security strategy model provides security to wireless local area networks," said a cell phone company executive. "It's a modern technology being used by the investigators across the world and that could only be done through cell phone Company's assistance. The police engage the companies in high-profile cases. The interior ministry has not yet allowed it but the police are implementing it by reaching an understanding with the companies" (Ayub 2015b).

The author of this magazine article reports that Geofencing technology, tracking the location of a mobile device, could offer an extra layer of security for enterprises trying to manage both company-owned and employee-owned devices. However, the technology can also raise worries about privacy and battery life. To counter this concern an extra layer of security, was added in the form of Geofencing to mobile device management software, tracking locations via GPS, Wi-Fi, and Bluetooth beacons. A similar approach could work in Wall Street firms where a Chinese firewall is supposed to be in place between certain departments. The CoSoSys Geofencing technology can tell which part of a building the employee is in. "Is there certain data that is not supposed to be accessed on the device while they have

the possibility to meet people from other areas?" he asked. This is not currently a regulatory requirement, he added, but might soon become one as the technology becomes more commonly available. A more common application is to use Geofencing to control access. "For example, it can be used to whitelist locations that authorized devices can be used from," said Talbot Harty, CEO at Fremont, Calif.-based Device Authority, Inc. "We have a few government agency projects underway which use this capability" (Korolov 2015).

The author of this magazine article discusses the various Geofencing constructs and concepts. Constructs are concepts, models, or schematic ideas: in their case they are the theoretical constructs of the Geofence used as a security strategy model. Their concept considers location-based services (LBS) and RFID as central to the security of wireless network security. Therefore location-based service and RFID technology emerge as key constructs. Using the Geofencing application framework, an organization can turn from less secure when it uses a wireless network to highly secure (Ijeh 2010b).

Published as a magazine article, its author discusses what occurs when devising wireless security strategies; network administrators must remain wary of "spoofing" assaults, a long-time practice where hackers hijack the communications of users who believe they're sending sensitive information on a secure pipeline. Defending against the vulnerability is complicated by the fact that wireless radio signals can travel through walls, leaving networks open to intrusions outside an organization's building. Start with enabling the encryption and authentication capabilities that come standard with switches and access points. IEEE-standard Wi-Fi Protected Access 2 (WPA2) uses Advanced Encryption Standard (AES) algorithms for powerful data encryption protections. Then take it a step further with measures for securing the areas where wired and wireless networks intersect. Special intrusion prevention systems for wireless environments can help network administrators quickly identify unauthorized devices trying to break through the security defenses. Wireless savvy IPS devices can also beat back denial-of-service attacks designed to crash networks. Geofencing (erecting a virtual perimeter around a geographic site) and other techniques grant access only to devices running at known and trusted physical locations. Administrators can create virtual LANs (VLANs) and regulate traffic using access control lists (ACLs) to guard against vulnerabilities that arise when guest users need to connect to the Internet over a wireless link. Alternately, a wireless LAN controller can be dedicated to this purpose and used to divert guest user traffic to a secure location outside the organization's firewall (Edtechmagazine 2015).

This magazine article looks at services available through Zippr relying heavily on Geofencing. When integrating with our partners, we urge them to specify areas to which they can fulfil orders to the best of their abilities, effectively and efficiently resulting in reduced order rejection rates and better customer service to our users through on-time deliveries and fulfilled orders. These specific areas are called "trade zones" and in this case when digitized are called "Geofences" or "Geographical fences" (Geofencing 2015).

Conference and Symposium Proceedings

Conference proceedings are important works for Geofencing researchers and practitioners. The following proceedings published papers citing Geofencing as security strategy model; most proceedings are less than 5 years. This conference paper looks at the success of disaster handling which often depends on the efficient flow of information. The social media and networks receive a growing attention as potential source of valuable data in disaster scenarios. The social network-based information flow is real time, direct, two-directional, and often geo-tagged. Unfortunately, besides these obvious advantages, social network data suffers from drawbacks: it is unstructured, dispersed, and lacks reliability. This paper proposes an approach based on combining a Geofencing technology with social network platform to combat this problem and deliver a novel service for disaster management. The service groups users ad hoc based on their location. Social network features allow users to exchange real-time information, coordinate rescue efforts, and issue reports. The Geofences are visualized to provide a good overview of the disaster zone. The service was evaluated by disaster management experts, with an encouraging feedback (Szczytowski 2015).

This conference paper looks at the modern smartphone, and car concepts provide a fertile ground for new location-aware applications, ranging from traffic management to social services. While the functionality is partly implemented at the mobile terminal, there is a rising need for efficient back-end processing of high-volume, high-update rate location streams. It is in this environment that Geofencing, the detection of objects traversing virtual fences, is becoming a universal primitive required by an ever-growing number of applications. To satisfy the functionality and performance requirements of large-scale Geofencing applications, we present in this work a back-end system for indexing massive quantities of mobile objects and Geofences. Our system runs on a cluster of servers, achieving a throughput of location updates that scale linearly with the number of machines. The key ingredients to achieve a high performance are a specialized spatial index, a dynamic caching mechanism, and a load-sharing principle that reduces communication overhead to a minimum and enables a shared-nothing architecture. The throughput of the spatial index as well as the performance of the overall system is demonstrated by experiments using simulations of large-scale Geofencing apps (Cirillo et al. 2014).

This conference paper looks at flash floods in Oman which is subject to major flash flooding which records show has occurred in Oman since 1989 to date. Whenever major flash floods occur in Oman, lives are lost, and infrastructure worth millions of Omani rials is destroyed. The purpose of this paper is to present findings from exploitation of geo-information systems and sensor technologies to mitigate risks to Oman's population caused by flash floods in Oman. Design/methodology/approach – The studies' approach uses system integration to adopt behavioral patterns inherent in geo-information systems and sensor technologies to provide a solution to flash flood challenges facing Oman's population. Findings: Preliminary findings from simulation of the framework suggest that the integrated system is able to mitigate the risks caused by flash flood facing Oman's population. Research limitations/implications: Findings are based on simulation of the

framework and not testing in a live environment. Future research could explore testing in a live environment. Practical implications: The implication of the findings is that it lays a foundation for academics and practitioners to develop a suitable prototype for mitigating flash flood risks to Oman's population. Originality/value: The value of the paper is that it presents a novel solution to flash floods which are a major national challenge facing Oman's population (Ijeh 2016).

This conference paper reports that social networks are unequivocally the most used application for communication and information sharing in the twenty-first century. As growth of this technology increases, there is a need to implement a more secure authentication mechanism to protect users as well as the platform providers from various social engineering attacks. A recent study from LinkedIn and Twitter hacks shows that weak passwords and single-factor authentication are still prevalent shortcomings facing most social networking sites. This end-user security lapse often paves way for phishing and malware attacks and undermines the overall integrity of the system. In this study, we review the rise of social networks and the underlying concepts of two-factor authentication. Furthermore, we propose a novel, feasible, cost-effective, and secure technique of applying an e-mail-based password tokenization as a second factor authentication in social networking sites (Ikhalia and Imafidon 2013).

Industry Expert Evaluation

Demonstration of Geofencing as a Security Strategy Model [oral presentation] SITC Innovation Showcase and Networking Dinner, held at the DCC Academy, Shrivenham, UK [25 March 2010] Ijeh (2010c): "It's a good innovation with a wide variety of applications" (Deputy CEO, SITC). Swain (2010): "We have a need for flexible technology like this" (Chief Executive Officer SITC and former Head of Metropolitan Police International Counter Terrorist Unit). Tyler (2010)): "With this application we can do so many things in making life easier for the elderly who we are currently focused on" (Technology Strategy Board: Innovation Platform Leader on Network Security). Churchill (2010)): "It's great to see so much innovation coming through from the research industry" (Government consultant and founding member of the Technology Strategy Board). Pragnell (2010)): "We have a need for the technology in a program we are currently undertaking" (ExactTrak and Home Office). Meston (2010)): "The technology can be used to protect equipment from unwanted signal interference" (Thales UK). Wynd (2010)): "We can use the technology to pinpoint and monitor or control communication ability under surveillance" (Thales UK). Fisken (2010)): "We have technology that we are currently developing to perform similar functions to what your technology does" (Vice President EMEA, ARUBA Networks). Mullin (2010)): "The technology is definitely applicable in so many ways within the defence industry" (Manager, Investment in Innovation BAE Systems). Anon (2010): "The technology is obviously beneficial, you should seek funding from the relevant government bodies to commercialise it" (CPNI, Government Representative).

Limitations of the Study

Research impact assessment is not a novel endeavor, and usually assessments are done using a triangulation of methodologies. The methodology used in this study has placed reliance on bibliometric methods to assess research impact of a particular study's societal impact over a 10-year period. Bibliometric methods are frequently used to provide quantitative analysis of academic literature and to explore the impact of their field or of a particular paper.

Research that is highly cited or published in top journals may be good for the academic discipline but not for society. It takes years, or even decades, until a particular body of knowledge yields new products or services that affect society. This paper adds value to academia and practice by undertaking a publication analysis of a key reference work's output and its impact on society. However publication analysis is based on an author's citation of papers which is done for various reasons including referencing a particular methodology, demonstrating that an example has been used before, acknowledging their supervisors or experts in the field. Therefore the reason for the citation may not have commonality even in highly cited papers. From existing literature citation, counts only measure the usefulness of papers to other authors and nothing else. Innovation or genius of the concept presented is not measured; therefore the number of citations received by a paper has nothing to do with the content of the paper but is rather a survey of the usefulness of paper to other authors in the course of their work.

Conclusion: Summary, Challenges, and Future Directions

In the future this study could be strengthened by interviewing end users of the research to find out about their own experiences and gain insight into their own perspectives. If it were at all possible, technological forecasting prelaunch would be extremely beneficial for academics and practitioners rather than bibliometric analysis which evaluates studies postlaunch. As a Security Strategy Model, Geofencing provides innovative tracking and access control which has wide ranging uses such as providing real-time location information and monitoring to surveillance and security. In all, forty-seven articles were cited in this study which can be used a platform for future work on design and development of further Geofencing models. Literature shows that the original model was created in 2007 by a researcher at University of East London, for use in the National Health Service for securing mobile devices. Versatility of the model has enabled its adoption for various applications and in different industries and this trend is likely to continue.

Cross-References

- ▶ Cyber-Challenges and NATO
- ▶ Cyber-Security and Sustainable Development: The Case of Dubai
- ▶ Cyber-Security Policies of East European Countries

► Focusing on Mission and Business Objectives Through a Different Lens: The New Cyber Offensive
► Privacy in the Cyberspace: Threats and Prospects
► Protective Function of Digital Forensics

References

Akshay, S., & Apoorva, P. (2014) Security measures on mobile technology using software as a service. *International Journal of Science and Research*, *3*(7). Available at https://www.researchgate.net/publication/318420882_Security_Measures_on_Mobile_Technology_Using_Software_as_a_Service_SaaS. Accessed 25 Mar 2018.

Anon. (2010). The technology is obviously beneficial, you should seek funding from the relevant government bodies to commercialise it (CPNI, Government Representative). Demonstration of Geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com

Ayub, I. (2015a). Cell phone service providers agree to share data with police. (2015). [Blog] Dawn. Available at https://www.dawn.com/news/1196936. Accessed 23 Mar 2018.

Ayub, I. (2015b). Police manage to access cell phone users' data for high-profile cases. (2015). [Blog] Dawn. Available at https://www.dawn.com/news/1209575. Accessed 23 Mar 2018.

Biltgen, P. (2016). *Activity-based intelligence: Principles and applications (The Artech House Electronic Warfare Library)*. Artech House, Norwood, MA.

Boselli, C., Danis, J., McQueen, S., Breger, A., Jiang, T., Looze, D., & Ni, D. (2016). Geo-fencing to secure airport perimeter against sUAS. *International Journal of Intelligent Unmanned Systems, 5*(4), 102–116. Available at: https://www.emeraldinsight.com/doi/pdfplus/10.1108/IJIUS-02-2017-0002. Accessed 25 Mar 2018.

Churchill, A. (2010). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Cirillo, F., Jacobs, T., Martin, M., & Szczytowski, P. (2014). Large scale indexing of geofences. Pdfs.semanticscholar.org. Available at https://pdfs.semanticscholar.org/0922/cc5c0b2420178a7de937b437d9e94eb6018d.pdf. Accessed 24 Mar 2018.

Dabhi, M. (2016). Geofencing: A generic approach to real time location based tracking system. [Online] Ijcnwc.org. Available at http://www.ijcnwc.org/papers/vol6no62016/6vol6no6.pdf. Accessed 24 Mar 2018.

Edtechmagazine.com. (2015). Resiliency, reliability and security are key concerns for maintaining network resources. Available at https://edtechmagazine.com/sites/default/files/88889-wp-g-networks-df.pdf. Accessed 23 Mar 2018.

Federal Register: The Daily Journal of the United States Government. (2015). Exemption to prohibition on circumvention of copyright protection systems for access control technologies. Available at https://www.federalregister.gov/documents/2015/10/28/2015-27212/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control. Accessed 24 Mar 2018.

Fernandez, R., & Birse, S. (2014). Branch device geo-fencing pairing security. US20160078742A1.

Fisken, D. (2010). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Foeckl, R. (2015). *Why geofencing will become the next endpoint security innovation* (Vol. 5, pp. 2–4). SC Media. Available at https://www.scmagazineuk.com/why-geofencing-will-become-the-next-endpoint-security-innovation/article/537168/. Accessed 24 Mar 2018.

Geofencing 101. (2015). A beginners guide. [Blog] Zippr. Available at http://zip.pr/blog_full.php?id=1440060061. Accessed 26 Mar 2018.

Grosinger, M., & Hackett, C. (2014). *The growth of geofence tools within the mapping technology sphere* (Vol. 12, pp. 2–5). Available at https://www.pdvwireless.com/the-growth-of-geofence-tools-within-the-mapping-technology-sphere/. Accessed 24 Mar 2018.

Haddock, W. J. (2016). Geo-fencing technologies and security. Geo-fencing technologies and security. InfoSecWriters.com. Available at http://www.infosecwriters.com/articles/2016/06/27/geo-fencing-technologies-and-security. Accessed 24 Mar 2018.

HIPAA Journal. (2015). Mobile devices under HIPAA rules: Will geofencing boost data security. *HIPAA Journal*, 1–3. Available at https://www.hipaajournal.com/mobile-devices-hipaa-rules-geofencing-data-security-443/. Accessed 25 Mar 2018.

Ijeh, A. (2010a). Wireless security model. *IPO UK Journal 6342*, GB1018091.7.

Ijeh, A. (2010b). Geofencing security engineering. In: *International multiconference of engineers and computer scientists* (pp. 1–6). Hong Kong: IAENG. Available at https://pdfs.semanticscholar.org/21d5/409fd2087d1f8e311574a100dfd61cbca269.pdf. Accessed 25 Mar 2018.

Ijeh, A. (2010c). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Ijeh, A. (2011). *Geofencing as a security strategy model*. Professional Doctorate, University of East London.

Ijeh, A. (2015). Geofencing as a tool for participatory processes. In O. Saar (Ed.), *E-governance and urban policy design for developing countries* (15th ed., pp. 132–143). Nairobi: UN Habitat. Available at https://unhabitat.org/books/e-governance-and-urban-policy-design-in-developing-countries/. Accessed 25 Mar 2018.

Ijeh, A. (2016). Exploiting geographic information systems and remote sensing for flash floods in Oman. In *International water conference 2016 on water resource in arid areas: The way forward* (pp. 1–15). Muscat: Springer. Available at https://conference.squ.edu.om/Portals/49/AbstractBook.pdf. Accessed 25 Mar 2018.

Ijeh, A., Brimicombe, A., Preston, D., & Imafidon, C. (2009). Geofencing in a security strategy model. In *International conference on global security, safety, and sustainability* (pp. 104–111). Berlin: Springer. Available at https://link.springer.com/chapter/10.1007/978-3-642-04062-7_11. Accessed 24 Mar 2018.

Ikhalia, E. (2013). A new social media security model (SMSM). *International Journal of Emerging Technology and Advanced Engineering, [online], 3*(7), 1–6. Available at https://pdfs.semanticscholar.org/1e8f/a1a62da5e714efced6396927aa2c9afa1192.pdf.

Ikhalia, E., & Imafidon, C. (2013). The need for two factor authentication in social media. In *Proceedings of the international conference on future trends in computing and communication 2013* (pp. 1–8). Bangkok: International Conference on Future Trends in Computing and Communication. Available at https://www.researchgate.net/publication/256667821_The_need_for_two_factor_authentication_in_social_media. Accessed 24 Mar 2018.

Jaltare, P., & Holey, A. (2016). Study of location tracking in geo-fencing services. *International Journal of Advanced Innovative Technology, 1*(2), 1–4. Available at http://www.garph.org/downloads/PGDCST_HVPM_IJAITE_SPECIAL_ISSUE/40.pdf. Accessed 25 Mar 2018.

Johansmeyer, M. (2013). *Securing public safety vehicles: Reducing vulnerabilities by leveraging smart technology and design strategies*. MSc, Naval Postgraduate School.

Korolov, M. (2015). *Geofencing could add security layer for mobile devices* (pp. 1–4). CSO. Available at https://www.csoonline.com/article/2891834/mobile-security/geofencing-could-add-security-layer-for-mobile-devices.html. Accessed 25 Mar 2018.

Long, D. (2013). Remote HMI panel having location based operational restrictions IN World Intellectual Property Organisation. WO/2013/191684.

Luxhoj, J. (2016). System safety modeling of alternative geofencing configurations for small UAS. *International Journal of Aviation, Aeronautics, and Aerospace, 3*(1), 1–27. Available at https://commons.erau.edu/cgi/viewcontent.cgi?article=1105&context=ijaaa. Accessed 25 Mar 2018.

Marchetti, J. (2014). Wearable-home integrated technology (WHIT) Project EDSGN 100, Section 009.

Marie, M. (2014). Indoor and outdoor social alarms: Understanding users' perspectives. *JMIR mHealth and uHealth, 2*(1), 1–6. Available at https://mhealth.jmir.org/2014/1/e9/. Accessed 25 Mar 2018.

Meston, J. (2010). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Modali, P., Gadamsetty, U., & Wei, J. (2014). Context aware Geofencing related applications. WO2014200504A1.

Mullin, D. (2010). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Muriach, A. (2015). *Information provision improvement with a geofencing event-based system*. MSc, Universitat Jaume I Castelló, Spain.

Osborne, P.. (2010). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Parab, N., Koukoumidis, E., & Bryar, N. (2013). Geofence compositions. US20150148060A1.

Prabu, A., Kodavati, B., Appa Rao, T., Rambabu, E., & Sundar Tripathy, S. (2011). Telematics based security system. *International Journal of Wireless & Mobile Networks (IJWMN), 3*(2), 1–10. http://airccse.org/journal/jwmn/0411wmn12.pdf. Accessed 25 Mar 2018.

Pragnell, J. (2010). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Rahate, S., & Shaikh, M. (2016). Geo-fencing infrastructure: Location based service. *International Research Journal of Engineering and Technology (IRJET), 3*(11), 1–4. Available at https://www.irjet.net/archives/V3/i11/IRJET-V3I11194.pdf. Accessed 25 Mar 2018.

Swain, S. (2010). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Szczytowski, P. (2015). Geo-fencing based disaster management service. In *Agent technology for intelligent mobile services and smart societies* (Vol. 498, pp. 11–21). Berlin: Springer. Available at https://link.springer.com/chapter/10.1007/978-3-662-46241-6_2. Accessed 25 Mar 2018.

Tyler, A. (2010). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Van Raan, A. F. J. (2003). The use of bibliometric analysis in research performance assessment and monitoring of interdisciplinary scientific developments. *Technikfolgenabschätzung-Theorie und Praxis/Technology Assessment-Theory and Practice, 1*(12), 20–29.

Veira, M., & Tsotras, V. (2013). Flexible pattern queries. In M. Veira & V. Tsotras (Eds.), *Spatio-temporal databases* (1st ed., pp. 5–35). Berlin: Springer. Available at http://www.springer.com/gp/book/9783319024073. Accessed 25 Mar 2018.

Wynd, S. (2010). Demonstration of geofencing as a security strategy model at SITC innovation showcase and networking dinner, held at the DCC Academy, Shrivenham, UK. http://securityintech.com.

Zin, M., Nurji, M., Isa, A., & Isa, M. (2016). Geofencing-based auto-silent mode application. *Journal of Telecommunication, Electronic and Computer Engineering, [online], 8*(10), 1–6. Available at http://journal.utem.edu.my/index.php/jtec/article/viewFile/1398/880. Accessed 25 Mar 2018.

Index

E. G. Carayannis et al. (eds.), *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, https://doi.org/10.1007/978-3-319-09069-6