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

Cyber-Development, Cyber-Democracy and Cyber-Defense

Challenges, Opportunities and Implications for Theory, Policy and Practice

Springer

Cyber-Development, Cyber-Democracy and Cyber-Defense

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

Cyber-Development, Cyber-Democracy and Cyber-Defense

Challenges, Opportunities and Implications for Theory, Policy and Practice

Springer

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

Marios Panagiotis Efthymiopoulos
Harriman Institute
Columbia University & Strategy
International
New York, NY, USA

David F.J. Campbell
Faculty for Interdisciplinary Studies
Institute of Science Communication
and Higher Education Research
University of Klagenfurt
Klagenfurt, Austria

Department of Political Science
University of Vienna
Vienna, Austria

ISBN 978-1-4939-1027-4 ISBN 978-1-4939-1028-1 (eBook)
DOI 10.1007/978-1-4939-1028-1
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2014942518

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This publication focuses on a new approach in interdisciplinary and transdisciplinary research. ***Cyber-Development***, ***Cyber-Democracy and Cyber-Defense*** are placed within a comparative framework of analysis, which is interested in inquiring further the involved challenges, opportunities, and implications for theory, conceptual evolution, policy, practice, and learning. The unfolding dynamics of the revolution of knowledge production, innovation application, and IT (information technology) poses dramatic changes on development, democracy, and defense. Cyber-Development, Cyber-Democracy and Cyber-Defense reflect as a term and concept this transformation. The joint phrase of "Cyber" should express and emphasize that the processes that drive development, democracy, and defense are in fact interrelated, they cross-link, overlap, and network with each other. *A new complexity of Cyber and in Cyber emerges. This stretches our thinking and our practice to a new Cyber-Horizon beyond established structures*.

Washington, DC, USA — Elias G. Carayannis
Klagenfurt, Austria — David F.J. Campbell
Vienna, Austria
New York, NY, USA — Marios Panagiotis Efthymiopoulos

Contents

About the Editors

Elias G. Carayannis is Full Professor of Science, Technology, Innovation and Entrepreneurship, as well as Cofounder and Codirector 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, DC. Dr. 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. He is fluent in English, French, German, Greek, and has a working knowledge of Spanish. For more information see: http://business.gwu.edu/faculty/elias_carayannis.cfm; E-mail: caraye@gwu.edu.

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://uni-klu.ac.at/wiho/inhalt/876.htm); Lecturer in Political Science at the University of Vienna (http://politikwissenschaft.univie.ac.at/institut/personen/lektorinnen/); and Quality Enhancement Manager and Quality Researcher at the University of Applied Arts in Vienna(http://www.dieangewandte.at/jart/prj3/angewandte/main.jart?rel=de&content-id=1268829109404&reserve-mode=active). He studied political science at the University of Vienna and finished with a doctoral degree in 1996. Campbell can be reached at: david.campbell@uni-klu.ac.at or david.campbell@uni-ak.ac.at.

Marios Panagiotis Efthymiopoulos is the CEO and Founder of the Think Tank Strategy International. A Visiting Scholar at Columbia University, Harriman Institute, he holds a Ph.D. in Political Science and Strategic Affairs from the University of Crete. A Masters in Advanced International Affairs from the Diplomatic Academy of Vienna, following a year to the London School of Economics and Political Science's masters in Russian and Post-Soviet Studies, and a B.A. (Hons.) from the University of Lincolnshire and Humberside in Politics and International Relations. Dr. Efthymiopoulos is an expert in Negotiations and

Strategic diplomatic affairs. Dr. Efthymiopoulos is an analyst and contributing author and lecturer to a majority of journals, think tanks, government training institutions, international organizations. He is a strategist and communication expert. His expert views are constantly seen on national and international media. Dr. Efthymiopoulos previous engagements, included positions at the Center for Transatlantic Relations at SAIS, Johns Hopkins University in Washington DC, the George Washington University, EU Center for Excellence, in Washington, DC, and the Woodrow Wilson International Center for Scholars, Washington, DC. He was a visiting Lecturer at the Department of Social and Political Sciences, University of Cyprus, Nicosia, Cyprus, and a variety of international organizations training institutions national and international. He has extensive professional experience with International organizations such as the UN and NATO and government political and international affairs through his works in Greece and the USA. Dr. Efthymiopoulos is listed in the Marquis Who is Who, in the World.

About the Contributors

Ian Ahl has provided services related to Information Technology and Information Security for over 10 years. Ian is currently a Senior Incident Response (IR) consultant for FireEye. He provides IR services to several high profile clients. An avid educator, Ian has delivered classes to thousands of students at various venues on Information Security topics. Ian participates heavily in the Open Source community where he has written whitepapers, articles, and programs. Several of these programs have been adopted into linux distributions such as Kali, and HoneyDrive. Ian holds a Master's degree in Information Technology, and an Information Security from American InterContinental University (AIU) and a Bachelor's degree in Information Technology. He also holds an Associate's degree in Business Administration from AIU. His certifications include CISSP, C|EH, MCPS – ePO, MCPS & HIPs.

Thorsten D. Barth is a political scientist (graduated with a dissertation, Dr. phil., from the University of Vienna, Austria) and a graphic designer in Austria. His research interests are civic education, the quality of democracy and information design. See for more information: http://democracyranking.org or http://visual.ly/users/drbarth.

Johanna Diecker is working as a freelance researcher and as a project manager in international development. She has a keen interest in the EU and democratization processes, especially with regards to the potential of Information and Communication Technologies (ICT). Having worked for the GIZ in the ICT for Development sector project, she is also curious on how to translate experiences to developing democracies. She holds a M.A. degree in political sciences and a B.A. degree in development studies. E-mail: johanna.diecker@gmx.de.

Matthias Galan is working in the communications sector. He is mainly interested in the relation between the EU institutions and citizens. In his work he focuses on the translation of complex EU-related issues into media-compatible and citizen-friendly information materials. Matthias holds a M.A. degree in political sciences and a B.A. degree in development studies. As a freelance researcher, he is interested in concepts of democratic legitimacy and political communication from a normative and empirical perspective. E-mail: matthias.galan@gmail.com.

David Koranyi Under-Secretary of State of Hungary, is a Nonresident Fellow at the SAIS Centre for Transatlantic Relations. He was previously a Visiting Research Fellow at CTR in 2010–11. His research is on Central European and Transatlantic energy security issues. As Under-Secretary of State, David Koranyi served as the chief foreign policy and national security advisor to the Prime Minister of the Republic of Hungary, Gordon Bajnai, in 2009–2010. He worked in the European Parliament as chief foreign policy advisor and head of cabinet of Hungarian MEP Csaba Tabajdi between 2004 and 2009. Previously he was a political advisor at the Hungarian National Assembly and a junior researcher at GKI Economic Research Institute, a Hungarian research firm. Mr Koranyi pursued undergraduate studies in political economy and business administration then obtained a Master's degree in International Relations and Economics, with a major in Foreign Affairs at Corvinus University from the Corvinus University of Budapest. He also studied law for eight semesters. Mr. Koranyi has published articles and studies on energy security, Hungarian and U.S. foreign policy, European integration, the Western Balkans and the United Nations. He edited a book titled "Transatlantic Energy Futures – Strategic Perspectives on Energy Security, Climate Change and New Technologies in Europe and the United States" published in December 2011 by Johns Hopkins SAIS CTR. Mr. Koranyi is a regular speaker at international conferences on foreign and security policy and energy security. He was a member of the Hungarian NATO Strategic Concept Special Advisory Group, a recipient of the German Marshall Fund's 2010 Marshall Memorial Fellowship and MMF Selection Board Member in 2011 and recipient of the French Foreign Ministry Fellowship in 2012. He is currently based in Budapest, Hungary. E-mail: david.koranyi@gmail.com.

Kostas Lavdas is Professor of European Politics and Director of the Centre for Political Research and Documentation (KEPET) at the University of Crete, where he was previously Vice-Rector for Academic Affairs and Personnel and Dean of the Faculty of Social Sciences. Born in Athens in 1964, he studied political science, political sociology, public policy and international relations in Athens, the UK (at LSE and Manchester), and the USA (at MIT). He has published extensively in English, German, and Greek on European politics, Greek politics and policy, comparative interest group politics and applied political theory. He has taught (as a Professor, an Associate Professor and a Senior Lecturer) and researched (as a Senior Research Fellow and a Research Associate) at several universities and research centers in Europe and the USA.

Fabio Liberti is a senior research fellow at the Institute for International and Strategic Relations (IRIS), where he is in charge of the different issues related to the functioning of the European Union, which encompasses: the Institutional Process, major European Common Policies. Expert on the Defence Policy of major EU Member States, as well as on the European Defence Technological and Industrial Base (EDTIB) and Armaments Programs, Fabio Liberti contributes in many Research Studies with regard to the European Common Security and Defence Policy headed by the European Defence Agency and the European Commission. Furthermore, he carried out several studies and he wrote various reports for the

French Ministry of Defence. Fabio Liberti is the Head Department of the IRIS Sup Diploma « Défense, Sécurité, Gestion de crises ». Beyond, he is responsible for the European issues publication in the Strategic Yearbook published by the IRIS. Fabio Liberti is a graduate of the Università degli studi di Napoli "L'Orientale," in the course of studies "Scienze Internazionali e Diplomatiche," specializing in Politics and Economic Geography, with a focus on European Industries and Policies in the Defence Sector. Moreover, he obtained a master's degree in Geography of the University Paris XII of Marne-la-Vallée. E-mail: liberti@iris-france.org.

Birgit Mitterlehner is the head and a researcher at the P/S/R Institute—an interdisciplinary research institute, specialized in social and legal sciences—in Vienna. She studied political science, translation and interpretation at the University of Vienna. In her studies, she focused on law and economics as well as the European Union. At present, she studies law at the University of Linz and completes her Ph.D. in Interdisciplinary Legal Sciences at the University of Vienna. At the P/S/R Institute, Mitterlehner in charge of Welfare States and Europe, European Law, particularly Competition law and Data Protection law. She has carried out European comparative studies in the field of critical infrastructure, notably ICT, transport and regional supply. Besides publications in journals and the P/S/R publication series, she has been working as a reviewer for Axel Springer New York and as a freelance translator and interpreter. She can be reached at: bmitterlehner@psr-institut.at or birgit.mitterlehner@outlook.com.

Nikitakos Nikitas is a graduate of Hellenic Naval Academy (1980) and holds a B.Sc. in Economics (University of Piraeus 1986) and two M.Sc. from Naval Postgraduate School, Monterey, CA, USA (M.Sc. Electrical Engineering. and M.Sc. in Appl. Mathematics). He spent 25 years as Naval Officer (Captain H.N. ret.) when he participated in several NATO and EU committees. He is decorated with ten national and international metals among them the medal for Kuwait's liberation and King Fahd's medal of Saudi Arabia for his participation in operation Desert Storm He received a Ph.D. in Electrical and Computer Engineering from National Technical University of Athens (1996). He has participated mainly as coordinator/principal researcher in several European and defense-related research projects. He was AMMITEC's (Association of Maritime Managers Information Technology Electronics and Communication) president from 2006 to 2010 and currently President of Aegean Institute of the Law of the Sea and Maritime law in Rhodes. He holds three international patents on renewable energies at sea and he was awarded from Lloyd's List on Maritime Technological Innovation in 2006. He has published five books and many articles in international referred journals and conferences.

Mavropoulos Panos Lt Gen (ret) *Mavropoulos*, Born on 17 December 1956, graduated from the Hellenic Army Academy in 1978, when he was commissioned as an Officer. He earned his Master's (with distinction) and Engineer's degrees in Electronic Engineering from the US Naval Postgraduate School in 1988. He also earned a Master's degree in National Security Strategy from the US National Defense University (War College) in 2004. He served four tours in NATO posts, as

operations staff officer, Contingency Operations strategic planner at SHAPE, Chief of Staff of JFTC in Poland and commander of NATO's Communications Zone South (COMMZ(S)). Since 2009 he teaches *Theory of War and Strategy* at the Hellenic Army Academy.

Tuğba Özcan is a Political Scientist in Vienna, Austria. Her E-mail address is: tuba_oezcan@hotmail.com.

Pythagoras Petratos is a Departmental Lecturer at Saïd Business School, University of Oxford. His studies include postgraduate degrees from Cass Business School, City University, University of London and the University of Oxford in Finance, Economics (Health), European Politics and Computer Science (Engineering) respectively. He was awarded his Ph.D. from the University of London. Pythagoras is listed in the Marquis Who is Who in the World and was recognized as a Distinguished Scientist by the Greek State. He was also elected Fellow of the Royal Society for the encouragement of Arts, Manufactures and Commerce. He has taught undergraduate and postgraduate courses at the University of London, ESCP Europe, University of Buckingham, and numerous Greek Universities and faculties (Economic Departments, Medical Schools, Social Science) as a Visiting Professor. He was a Visiting Fellow at Cambridge University for the period 2006–2008. E-mail: p.pythagoras@yahoo.com.

Willi Schlegelmilch is employed as a manager in the automotive industry (in Germany). He holds responsibility for designing and implementing purchasing, invoicing and accounting processes for a worldwide sales organization. His research interests are the quality of democracy, information management and system design.

Dan Solomon is a senior partner at Hawk ISM. He is heading the security consulting and risk practice. He is an experienced strategy consultant, and former VP of Consulting, regularly presenting and publishing on converged risk, cyber security, critical infrastructure protection, open source intelligence, and red teaming. He is also the Director of the Homeland Security program at the Atlantic Council of the United Kingdom. E-mail: d.solomon@hawk-ism.com.

Zenonas Tziarras is a graduate of the Department of Mediterranean Studies at the University of the Aegean, Rhodes (Greece) where he specialized in International Relations and Organizations. His dissertation titled "Turkey's Accession Process to the EU and the Cyprus Problem" gained a distinction. He continued his studies at the University of Birmingham and received an M.A. in International Relations and Strategic Studies. During his Masters program he also attended specialization courses in International Security at the University of Delhi, India. His M.A. dissertation was titled "The Changing Role of Ethnicity in Ethnic Conflicts: The Cases of Cyprus and Sri Lanka," and also gained a distinction. He is currently a final year Ph.D. Candidate and Teaching Assistant in the Department of Politics and International Studies at the University of Warwick, UK, and a Nonresident Research Scholar at the think tank Strategy International. He works under the supervision of Dr. Nicola Pratt and Dr. George Christou while his research focuses on Turkish

foreign policy under the AKP towards the Middle East and employs a Neoclassical Realist analytical framework. Further, he has been research assistant in programs on conflict analysis and resolution, completed an internship at the Peace Research Institute of Oslo Cyprus Centre, attended training courses in Leadership and Conflict Resolution at Koç University, Istanbul, Turkey, and he is the cofounder and coeditor of the online magazine *The Globalized World Post*. He is a frequent commentator on Middle East and Mediterranean political affairs and has presented his work at conferences in Cyprus, Greece, Turkey, Poland, and the UK.

Stilianos Vidalis was born in Athens, Greece, and raised on an island in the Aegean Sea. He moved in Wales in 1995 where he did his undergraduate and postgraduate studies. He received his Ph.D. in Threat Assessment in July 2004. He joined the University of Wales, Newport in 2006 where he is currently employed as a Senior Lecturer. He is the Head of the Centre for Information Operations and the program leader for the B.Sc. Computer Forensics, and B.Sc. Information Security. Dr. Vidalis is a member of the BCS South Wales Committee, a member of the E-Crime Wales Steering Group, and a member of the Military Educational Committee of the Welsh OTC. He is also a panel member for the International Conference of Information Warfare and for the European Conference of Information Warfare and Security. His research interests are in the areas of Information Security, Information Operations, digital forensics, threat assessment, and effective computer defense mechanisms. E-mail: Stillianos.Vidalis@newport.ac.uk.

Robert F. Xavier is a pseudonym. Xavier is a blogger and independent analyst of Middle Eastern affairs. Formerly operating under his real name, Xavier ran a geo - political news blog on the Middle East and continues to write on several topics related to the region. In 2009, Xavier covered the Iranian Presidential Elections and the Lebanese Parliamentary Elections through live blogging. Xavier intends on launching a new blog covering the Middle East. E-mail: rfrxavier@gmail.com.

Part I
Cyber-Development

Elias G. Carayannis

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[1]. Moreover, there are strong indications and emerging trends that there are qualitative and quantitative differences between the twentieth and the twenty-first century drivers of economic growth[2]:

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.

We are currently going through a dynamic era for the economies of the world where a country can transition fast both upwards and downwards, and this trend has become increasingly more pronounced and in an accelerating fashion during the last decade. This new era is punctuated by[3]:

- 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.

[1] The Global Competitiveness Report 2001–2002, WEF & Harvard CID, NY/Oxford, OUP, 2002.

[2] Toward e-Development in Asia and the Pacific: A Strategic Approach for Information and Communication Technology, ADB, June 2001.

[3] China and the Knowledge Economy: Seizing the 21st Century, Carl Dahlman & jean Eric Aubert, WBI, October 2001.

- 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 2002, 2005).

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 (Carayannis 2002, 2005). This also applies to the advanced economies.

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 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.

Chapter 1
From Development as Democracy to Innovation as Development

Elias G. Carayannis

Abstract Current local, regional, and global economic and financial conditions and trends make the need to trigger, catalyze, and accelerate high quantity and quality entrepreneurial initiatives that are based on high quality and quantity innovations. Given the uncertainty and change inherent in the innovation process, management must develop skills and understanding of the process a method for managing the disruption. Technology changes the way society functions. The dramatic advances in technology over recent decades have collaterally precipitated wide sweeping and profound change to the functioning of almost every form of human exchange, the world over. Income inequality in the USA has being growing since the late 1970s, but easy credit and rising asset prices had allowed American households to increase financial leverage to finance consumption. Now an increasing number of academics and intellectuals recognize that the growing income inequality is one of the key aspects behind the financial crash. The first step in understanding how the income redistribution can lead to innovation and help an economy move from a stagnant state into a new sustainable economic growth path is to understand how long-term trends in rising and falling income inequality affect the market environment that firms must survive in. In the late twentieth and the beginning of the twenty first century, numerous scholars and practitioners such as Peter Drucker have identified knowledge as perhaps the sixth and most important key input and output factor of economic activity.

Keywords Democracy • Development • E-development • Equality • Innovation • Sustainable development • Technology

E.G. Carayannis (✉)
Department of Information Systems and Technology Management,
School of Business, George Washington University,
Suite 515C, Funger Hall, 2201G Street NW, Washington, DC 20052, USA
e-mail: caraye@gwu.edu

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_1,

1.1 Introduction

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 innovation that unlocks and captures the pecuniary benefits of the science enterprise in the form of private, public, or hybrid goods (for instance, bio-entrepreneur-millionaires, knowledge for the public good—i.e., public health awareness, and new public–private research centers funded partly by bio-entrepreneur-millionaires and monies levied as taxes on bio-ventures).

Entrepreneurship and Innovation are human endeavors and socioeconomic phenomena that are *intrinsic to human nature* as well as constitute both social and political *engines of positive change and growth*, provided that they are balanced and guided by effective and transparent regulatory and incentive systems in place.

Current local, regional, and global economic and financial conditions and trends make the need to *trigger, catalyze*, *and accelerate high quantity and quality entrepreneurial initiatives* that are based on *high quality and quantity innovations* (low-tech, medium-tech, and high-tech) even more clear and present as this is one of the major ways and means to target and achieve *real, sustainable*, and *eventually accelerating GNP growth*. Such growth is much more likely to come from new and qualitative different and superior initiatives (from "sunrise" industries) rather than restructuring existing (and perhaps "sunset") industries. It may be strategically more prudent to invest scarce and precious resources in carefully calculated strategic "bets" rather than keep throwing them after waning industrial sectors and declining firms, and in that sense, it may be best to provide aggressive socioeconomic retraining, reinsertion, and/or early retirement programs to allow for real growth strategies to be implemented.

Moreover, we believe that the concepts of *robust competitiveness* and *sustainable entrepreneurship* (Carayannis, Elias G. 2008) are pillars of a regime called "*democratic capitalism*" (Carayannis and Kaloudis, 2010) (as opposed to "popular or casino capitalism"), where real opportunities for education and economic prosperity are available to all and especially the younger people (but not only the latter).

This would be the direct derivative of a collection of *top-down policies* as well as *bottom-up initiatives* (including strong R & D policies and funding but going beyond that to the development of *innovation networks and knowledge clusters across regions and sectors* (Carayannis and Campbell, 2006):

- We define *sustainable entrepreneurship* (Carayannis, 2008) as *the creation of viable, profitable, and scalable firms.* Such firms engender the formation of self-replicating and mutually enhancing innovation networks and knowledge clusters (innovation ecosystems) leading towards robust competitiveness.
- We understand *robust competitiveness* (Carayannis, 2008) as a state of economic being and becoming that avails systematic and defensible "unfair advantages" to the entities that are part of the economy. Such competitiveness is built on

mutually complementary and reinforcing low, medium, and high technology, public and private sector entities (government agencies, private firms, universities, and nongovernmental organizations). (see also excerpts from: http://search.barnesandnoble.com/Diversity-in-the-Knowledge-Economy-and-Society/Elias-Carayannis/e/9781847202116/?itm=5)

Existing and new small and medium enterprises (SMEs) that can provide better solutions for less will always be winners—even and perhaps especially in down markets and recessionary economic cycle stages—and this is the area where fiscal, monetary, institutional, intellectual property rights (IPR)-related and other public–private sectors programs and initiatives are needed to help unlock, capture, and leverage fully the value-adding potential of the Greek knowledge creation infrastructure (i.e., universities, research institutions, and private sector research and development (R & D) facilities) by providing incentives and establishing a large number, scale, and scope of pilots connecting organically and effectively all stages of the value adding knowledge chain (from the lab to the market via world-class SMEs that will be both locally and globally oriented by design and the new ones from their inception).

1.2 Innovation as Development

Discovery consists of looking at the same thing as everyone else and thinking something different.

Albert Szent-Györgyi—Nobel Prize Winner 1937

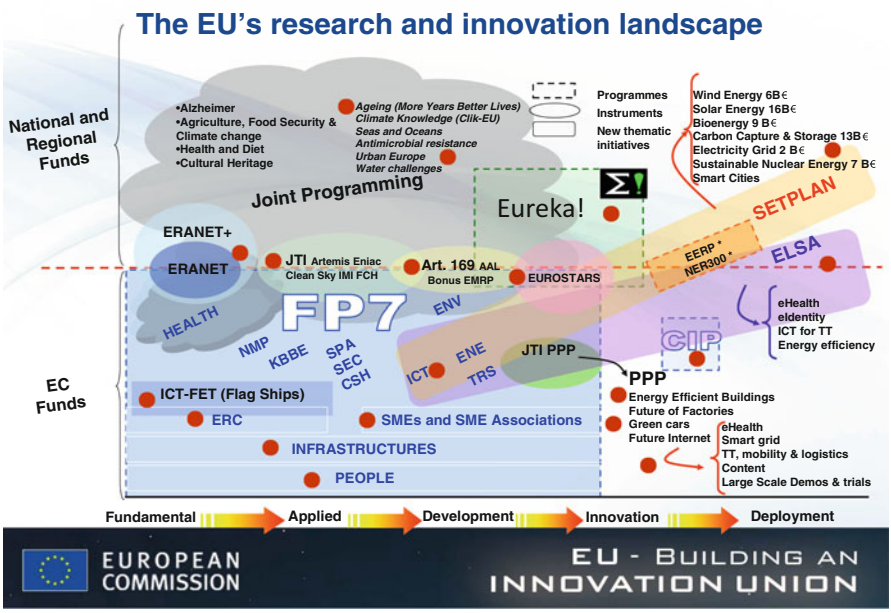

Fig. 1.1 Twenty-first century innovation ecosystem (Carayannis, Diversity in the Knowledge Economy and Society, Edward Elgar, May 2008)

Innovation is a word derived from the Latin, meaning to introduce something new to the existing realm and order of things or to change the yield of resources as stated by J.B. Say quoted in Drucker (Drucker, 1985).

In addition, innovation is often linked with creating a sustainable market around the introduction of new and superior product or process. Specifically, in the literature on the management of technology, technological innovation is characterized as the introduction of a new technology-based product into the market:

> *Technological innovation* is defined here as a situationally new development through which people extend their control over the environment. Essentially, technology is a tool of some kind that allows an individual to do something new. A technological innovation is basically information organized in a new way. So technology transfer amounts to the communication of information, usually from one organization to another. (Tornazky & Fleischer, 1990)

The broader interpretation of the term "innovation" refers to an innovation as an "idea, practice or material artifact" (Rogers and Shoemaker, 1971:19) adopted by a person or organization, where that artifact is "perceived to be new by the relevant unit of adoption" (Zaltman et al., 1973). Therefore, innovation tends to change perceptions and relationships at the organizational level, but its impact is not limited there. Innovation in its broader socio-technical, economic, and political context, can also substantially impact, shape, and evolve ways and means people live their lives, businesses form, compete, succeed and fail, and nations prosper or decline (see Fig. 1.1).

Specifically, Fig. 1.1 attempts to illustrate the nature and dynamics of an emerging globalization framework in which creativity and innovation—as enabler of technological effort in manufacturing and as an engine of industrial development—can lead to improved competitiveness and sustained development. On the other hand, lack of creativity and innovation constitutes a factor for failure in manufacturing

performance and, as a result, is a factor for failure in economic performance, too. For those countries in which creativity and innovation are applied effectively, globalization can be an engine of beneficial and sustainable economic integration. However, globalization can be a powerful force for deprivation, inequality, marginalization and economical disruption in those non-competitive countries.

Government or market success or failure is determined by how they take advantage of the four major elements that shape the setting for creativity, innovation and competitiveness in the globalized world: (1) The coordination and synergy in the relationship between governments, enterprises, research laboratories and other specialized bodies, universities and support agencies for small and medium enterprises (SMEs); (2) The power of information and communication technology; (3) The efficiency that managerial and organizational systems can bring to production and commerce; and (4) The international agreements, rules and regulations. All the four elements of this framework will impact on creativity and innovation at the micro level (firm level) as well as on innovation and competitiveness at the macro level (industry, national, global).

From a business perspective, an innovation is perceived as the happy ending of the commercialization journey of an invention, when that journey is indeed successful and leads to the creation of a sustainable and flourishing market niche or new market. Therefore, a technical discovery or invention (the creation of something new) is not significant to a company unless that new technology can be utilized to add value to the company, through increased revenues, reduced cost, and similar improvements in financial results. This has two important consequences for the analysis of any innovation in the context of a business organization.

First, an innovation must be integrated into the operations and strategy of the organization, so that it has a distinct impact on how the organization creates value or on the type of value the organization provides in the market.

Second, an innovation is a social process, since it is only through the intervention and management of people that an organization can realize the benefits of an innovation.

The discussion of innovation clearly leads to the development of a model, to understand the evolving nature of innovation. Innovation management is concerned with the activities of the firm undertaken to yield solutions to problems of product, process, and administration. Innovation involves uncertainty and disequilibrium. Nelson and Winter (1982) propose that almost any change, even trivial, represents innovation. They also suggest, given the uncertainty, that innovation results in the generation of new technologies and changes in relative weighting of existing technologies (ibid). This results in the ***disruptive process*** of disequilibrium. As an innovation is adopted and diffused, existing technologies may become less useful (reduction in weight factors) or even useless (weighing equivalent to "0") and abandoned altogether. The adoption phase is where uncertainty is introduced. New technologies are not adopted automatically, but rather markets influence the adoption rate (Carayannis, 1997, 1998). Innovative technologies must propose to solve a market need such as reduced costs or increased utility or increased productivity. The markets, however, are social constructs and subject to non-innovation related criteria.

For example, an invention may be promising, offering a substantial reduction on the cost of a product which normally would influence the market to accept the given innovation; but due to issues like information asymmetry (the lack of knowledge in the market concerning the invention's properties), the invention may not be readily accepted by the markets. Thus, the innovation may remain an invention. If, however, the innovation is market accepted, the results will bring about change to the existing technologies being replaced, leading to a change in the relative weighting of the existing technology. This is in effect ***disequilibrium.***

Given the uncertainty and change inherent in the innovation process, management must develop skills and understanding of the process as a method for managing the disruption. The problems of managing the resulting disruption are strategic in nature. The problems may be classified into three groups, ***engineering, entrepreneurial, and administrative*** (Drejer, 2002). This grouping correlates to the related types of innovation, namely, ***product, process, and administrative innovation***:

- *The engineering problem is one of selecting the appropriate technologies for proper operational performance.*
- *The entrepreneurial problem refers to defining the product/service domain and target markets.*
- *Administrative problems are concerned with reducing the uncertainty and risk during the previous phases.*

In much of the foregoing discussion, a recurring theme about innovation is that of ***uncertainty***, leading to the conclusion that an effective model of innovation must include a multidimensional approach (uncertainty is defined as unknown unknowns whereas risk is defined as known knowns). One model posited as an aide to understanding is the Multidimensional Model of Innovation (MMI) (Cooper, 1998). This model attempts to define the understanding of innovation by establishing three-dimensional boundaries. The planes are defined as product–process, incremental–radical, and administrative–technical. The product–process boundary concerns itself with the end product and its relationship to the methods employed by firms to produce and distribute the product. Incremental–radical defines the degree of relative strategic change that accompanies the diffusion of an innovation. This is a measure of the disturbance or disequilibrium in the market. Technological–administrative boundaries refer to the relationship of innovation change to the firm's operational core. The use of technological refers to the influences on basic firm output, while the administrative boundary would include innovations affecting associated factors of policy, resources, and social aspects of the firm.

1.2.1 Innovation Posture, Propensity, and Performance

We develop our conceptual model of organizational innovation from a resource-based perspective of the firm (Penrose, 1959; Barney, 1991). In particular, we draw upon the concept of knowledge as an intangible resource that flows throughout

organizations to render new routines, technologies, or structures that affect future performance (Nelson and Winter, 1982). In order to capture the multilayered influence of organizational innovation, we conceive our framework for innovation routines as a procedural model. We focus on intangible resources that contribute inputs to the innovation process. We examine the firm's capabilities for engaging in innovating activities and finally consider the range of organizational outputs from innovation that spans short-horizon outcomes to long-horizon lasting impacts.

This composite of measures is housed within a "3P" framework for organizational innovation. Innovation emerges from three critical firm-level factors: ***Posture, Propensity***, and ***Performance***.

- ***"Posture"*** refers to an organization's position within the greater innovation system of its environment (i.e., region, industry, technological domain). Specifically, Posture comprises a firm's state along three dimensions: the organizational, technological, and market life cycles, reflecting its readiness to both engage in and benefit from innovation (Damanpour, 1991). It thus identifies the conditions influencing a specific firm within a specific technology regime serving a specific market.
    - Each firm's ability to engage in innovative activities will be constrained by its Posture, which is exogenous to the innovation process being measured. That is, regardless of whether and what type of innovation process is employed, a firm exists at a point in its life cycle from formation to failure (organizational life cycle). The firm also selects technologies to employ in the implementation of its strategies and thus is subject to the state of the technology regime life cycle within which these technologies exist (technological life cycle).
    - For example, a handful of stagecoach companies continued operation for a period of time after the introduction of the automobile and thus their place in the stagecoach technology regime could be measured. Finally, the firm exists on a competitive landscape within significant strategic activities in one or more markets. These markets exist at various points in their own life cycle; therefore, they also constrain the innovative actions available to the firm.
- ***"Propensity"*** is a firm's ability to capitalize on its posture based on cultural acceptance of innovation. In this way, propensity is an intangible reflection of processes, routines and capabilities established within a firm. A firm may possess adequate resources and consequently higher externalized innovation stature, yet have an underdeveloped capacity for innovation due to cultural or other constraints.
- ***"Performance"*** is the lasting result of innovation. This part of the framework comprises three levels: output, outcome, and impact. Outputs occur as the immediate, internalized results of innovation. New product introductions, patents, and technology transfer licenses are among the outputs that emerge. Outcomes include mid-range results such as revenues contributed by new products. Finally, impacts represent more lasting, long-range benefits that accrue to the firm from its innovative competence and are transformed into results for the firm's environment too. Examples of impact performance include status as a top innovator in the industry.

All the three factors—Posture, Propensity, and Performance—are captured empirically in the form of a combinatorial we define as the ***Composite Innovation Index*** (CII). This comprehensive measure demonstrates the superior evaluative results of measuring innovation across all facets of its process in concert (Damanpour, 1991).

1.3 Development as Democracy

Technology changes the way society functions. The dramatic advances in technology over recent decades have collaterally precipitated wide sweeping and profound change to the functioning of almost every form of human exchange, the world over. What emerged in developed economies during the latter years of the twentieth Century is knowledge-based economics—an evolutionary framework of social transaction that now dominates the behavior of mankind in the twenty-first Century.

1.3.1 The Conceptual Framework of Knowledge Economy

> For countries in the vanguard of the world economy, the balance between knowledge and resources has shifted so far towards the former that knowledge has become perhaps the most important factor determining the standard of living – more than land, than tools, than labour. Today's most technologically advanced economies are truly knowledge-based. (*World Development Report, 1999*)

In classical economics, land, labor, and capital are the only factors of production. Knowledge, productivity, education, and intellectual capital are all regarded as exogenous factors, falling outside the system. The New Growth Theory recognizes two additional factors: technology, and the knowledge on which it is based. In today's environment, technology and knowledge are not merely additional factors of production; they have become the key factors of production. Knowledge is 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, in turn, are drivers of economic growth. Technology raises the return on investment, which is why developed countries can sustain growth and why developing economies cannot attain growth without it. Even with unlimited labor, natural resources, and ample capital, traditional economics predicts that there are diminishing returns on investment. New Growth theorists argue that the non-rivalry and technical platform effects of new technology can lead to increasing rather than diminishing returns on technological investment.[1] Investment can make

[1] The Ministry of Economic Development (2001). The Knowledge Economy: A submission to the New Zealand Government by the Minister for Information Technology's IT Advisory Group, August 1999—What Is the Knowledge Economy? Available: http://www.med.govt.nz/pbt/infotech/knowledge_economy/knowledge_economy-04.html.

technology more valuable and vice versa. The cycle that results can raise a country's growth rate permanently—which contradicts traditional economics.

Earning monopoly rents on discoveries is important to provide incentive to invest in R & D for technological innovation. This is why protection of Intellectual Property Rights (IPR) is fundamental to growth and traditional economics sees "perfect competition" as the ideal. Enhancing human capital is critical for GDP growth, as well. To make investments in technology, a country must have sufficient human capital. Human capital is defined as the formal education, training, and on-the-job learning embodied in the workforce.

"A knowledge-driven economy is one in which the generation and exploitation of knowledge play the predominant part in the creation of wealth" (UK Department of Trade and Industry, 1998). In contrast, during the industrial era, machines replacing human labor created wealth. Nowadays, many people associate the knowledge economy with high-technology industries such as telecommunications and financial services. Actually, knowledge workers are workers who manipulate symbols rather than machines. Architects, bank workers, fashion designers, pharmaceutical researchers, teachers, and policy analysts are all examples of knowledge workers. More than 60 % of US workers are knowledge workers. For knowledge workers, *know-why* and *know-who* matters more than *know-what*. Knowledge gained by experience is as important as formal education and training——lifelong learning is vital for organizations and individuals and its intellectual capital is a firm's source of competitive advantage.

The knowledge-based economy can be characterized as fractal. It is nonlinear, unstable, and stochastic. Like chaos theory, simple algorithms iterated successively yield very complex patterns and interrelationships, as epitomized by the butterfly flapping its wings in the Amazon to trigger a hurricane over the Atlantic months later. The knowledge-based economy creates profit avalanches. Entrance is easy for small, intelligent companies, but there is no space for organic growth; the market is instantly global and a newcomer can attain dominance in 10 years. It also differentiates itself by the convergence of technologies, which removes market sector boundaries: wireless, satellite, cable, and telecom no longer belong to discrete sectors. In a mobile information society, services as well are different, impacted by the presence of Internet, virtual organization, or network transactions. Information and Communication Technologies (ICTs) are enablers of change; they release creative potential and knowledge and open up global markets and foster competition. Network transaction economies resemble the most complex network: the human brain.[2] The digital revolution can be a great equalizer, but national policies must be right to enable it. Proper training and education can make a network transaction economy, or knowledge economy, more effective and efficient: *smarter*.

[2] Routti, Jorma (2003). Research and Innovation in Finland—Transformation into a Knowledge Economy. In *Competitiveness and the Knowledge Economy Research and Innovation Strategies: Cases of Chile and Finland*, presented at the Inter-American Development Bank, Washington, DC.

This elevation requires methodical enhancement of the business development environment, e.g., via business incubators. Advancement also requires enhancement of the network technology infrastructure, i.e., ICT. The state of the art is the virtual incubator, in which ICT extends and multiplies the effectiveness of business incubation at lower cost.

Regardless of externalities, each organization seeks to sustain itself in competition and cooperation with other entities that depend on the same finite pool of resources. The fundamental challenge is the very heart of economic discipline: ***the management and allocation of scarce resources***.

The advantage of the Knowledge Economy is that knowledge grows by sharing—donors do not forfeit what they know when passing knowledge to recipients, who in turn can share with others. The greatest phenomenon of knowledge-based economics is this multiplier effect: ***Sharing knowledge capital actually creates more of it.***

1.3.1.1 Public Policy

Governments have not surrendered their power to capitalism, even if the world's biggest companies are more powerful than many of the world's governments. *Democracy is not a sham. People rule, not profits. Admittedly though, companies would run the world for profit if they could. What stops them is not governments, but markets.* Economic parity arrives when technology allows people to pursue their own goals and they are given the liberty to do so. If technology can support trade across borders, and people choose to trade across borders, integration occurs. Because people have freely chosen it, the outcome is accepted, and because a free market is self-equilibrating, the trade precipitates economic benefits as well. Government must have a long-term commitment to building a market economy, and defending the mechanisms and protections in which a free market thrives.[3]

1.3.1.2 Public Practice

Technology-enabled free trade is an economic equalizer. Governments have power, but they do not always exercise it wisely. They are unreliable servants of the public interest. But limited government is not worth buying Markets keep the spoils of corruption small. Government that intervenes vigorously is worth a great deal. Especially in developing countries with weak legal systems, taming capitalism by regulation or trade protection often proves such a hazardous endeavor.

Central strategic planning works best from a demand-side intervention, enacting and enforcing regulations that enable people to get what they want, while protecting society from harmful, wasteful, or unfair practices.

[3] Ibid.

Historically what fails is central planning of supply-side regulations that specify what people may have, through prohibitions and licensing, by creating surpluses and shortages, or by setting quotas and prices to influence commerce and trade.

Distributed tactical planning works best under the control of the entrepreneurs, organizations, and actors operating in a free-market system. Government and NGOs function best when serving as facilitators and resources, not as managers and operators. If national governments or NGOs disable markets, the economic consequences can be dire, with direct spillover into political and social consequences. Governments must build transnational bridges of collaboration and cooperation, with immediate and long-term long commitment to building a market-oriented economy unimpeded by traditional boundaries.

1.3.1.3 Private Policy

Research and innovation must be managed today to secure sustainability for tomorrow. Open innovation is a policy of collaboration. Companies must manage intellectual property to manage research: they need to access external IP; they need to profit from internal IP. Researchers must be knowledge brokers as well as knowledge generators. Companies can profit from one another's IP. No one company has claim to all the smart people in a field. Competition and collaboration can and must coexist. Open innovation is knowledge diffusion and recombination, producing the "seed corn" of tomorrow's breakthroughs. Researchers must recognize their own potential, and be able to articulate possibilities to a receptive management for further development.[4]

Science-driven academic research is vital to returns. Scientists decide the basic research; industrialists decide the applied R & D. Management culture must encourage risk-taking. Fear of failure suppresses creativity and innovation, which undermines competitiveness. Failure is a great educator. Institutionally, a deviation from plan is an irregularity, but competitively it is creative, innovative, exploratory work. Creativity is essential.[5]

There is tremendous "white space" in market opportunities: new products, new processes, new markets, and new unknowns. Strategic community creation is a calculated alliance of many stakeholders to manage the white-space risk and facilitate adoption.

1.3.1.4 Private Practice

The priorities of new venture formation in the knowledge economy are: ICT and Internet access; linkages to investors and lenders; formation of lean management and advisory boards comprising experienced individuals, competent in their fields

[4] Chesbrough, op. cit.

[5] Routti, op. cit.

of discipline and having as few members as needed to get the job done; and planning and securing facilities.

The priorities of e-Development and sustained growth are as follows: the ability to evaluate and react to risk well; protection of product; stimulation of existing market; the available population of skilled knowledge workers—whether centralized in a physical facility or linked via a virtual organization.

All knowledge workers must have access to the Internet and competency in its use, ample training in computer literacy in addition to their specific technical expertise, and basic computer, math, and language skills. Firms must practice ongoing training to keep skills current; competitive advantage is volatile and requires constant reinforcement.

1.4 Income Inequality

Income inequality in the USA has been growing since the late 1970s, but easy credit and rising asset prices had allowed American households to increase financial leverage to finance consumption. "Let them eat credit" is how Raghuram Rajan summarizes how the political establishment dealt with the growing income inequality in America as he explains how income inequality is a fundamental cause of the current crisis in his book Fault Lines. With the mortgage crisis and the end of easy credit, the fractures in the economy were exposed. Just as Prof. Rajan, now an increasing number of academics and intellectuals recognize that the growing income inequality is one of the key aspects behind the financial crash.

Along those lines, this article also argues that reducing income inequality is a key part of the long-term resolution of this type of crisis. It explores the effects of income redistribution on businesses' innovative behavior, which is essential to helping spark and sustain economic growth.

1.4.1 Income Distribution, the Markets, and Firm's Innovation

The first step in understanding how the income redistribution can lead to innovation and help an economy move from a stagnant state into a new sustainable economic growth path is to understand how long-term trends in rising and falling income inequality affect the market environment that firms must survive in.

In that regard, observe that multinational enterprises (MNEs) are generally good at adapting to different market conditions around the globe to explore their knowledge based assets, and to create new knowledge based assets through innovation. Campino 2010 demonstrates that country income-level variations do impact foreign

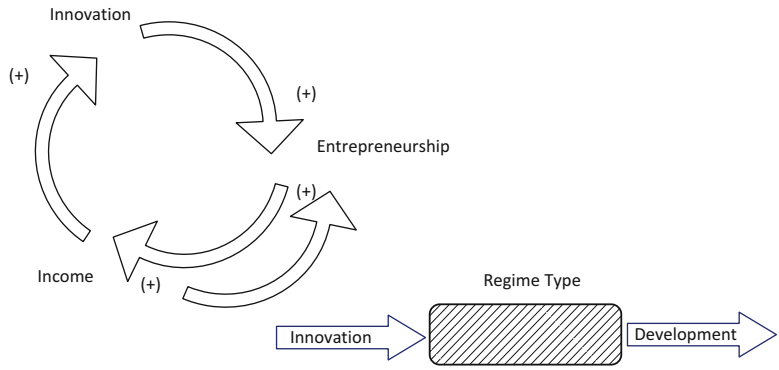

Fig. 1.2 Democracy, innovation development (DID) linkages

direct investments of MNEs, and that in particular MNEs' foreign direct investments behave in a manner that is consistent with that expected of high income elasticity of demand producers (i.e., luxury goods producers).

1.4.2 Preliminary Empirical Validation

At the macro level, innovation can translate into both top-down policies for a more efficient allocation of discretionary resources and a bottom-up increasing level of entrepreneurship. In addition, the type of regime under which a country operates can act as a catalyst or inhibitor of this process (see Fig. 1.2).

This article offers to explore the correlation between innovation and development. For this first attempt, we reduced development to only one of its numerous aspects: income distribution, which we in turn considered as an independent dependent variable.

At the firm level, innovation can be expressed in different ways depending on the time horizon. In the short-term, firm exhibit innovativeness; in the medium-term they exhibit different levels of innovative performance and in the long-term, different levels of innovative competence (Carayannis and Provance, 2007).

Both development and innovation are multidimensional concepts that cannot be easily captured in a single measure. For the purpose of this article, we measure one aspect of development as captured by the income distribution. We accept this limitation and hope to be able to expand our empirical model in future research. In this particular scenario, we were interested in the outcome of innovation, which we chose to proxy with the new-to-firm indicator of the European Innovation Scoreboard, as it measures the turnover of new or significantly improved products or processes to a firm.

Table 1.1 The new to firm measure

High income	*Lower middle income*
Austria	Bulgaria
Belgium	*Upper middle income*
Finland	Hungary
France	Latvia
Germany	Lithuania
Greece	Poland
Ireland	Slovak Republic
Italy	
Netherlands	
Portugal	
Slovenia	
Spain	
Sweden	
UK	

Regarding the New to Firm measure, the following results are for EU countries with a 3-year lag (Table 1.1). The New to Firm measure was available for 2004 and 2006 years only.

1.4.3 Hypothesis 1

Figure 1.3 shows the top 10 decile combinations ranked by R-square plus the combination containing all income-deciles (i.e., M_1023) obtained by regressing NewToFirm lagged by 3-years onto the GDP per-capita of 27 observations spanning 20 countries and 2-years.

There were 510 statistically significant decile combinations with R-square values higher than that obtained from the combination containing all income-deciles (i.e., M_1023) of 16.96 %. Therefore, with regards to H1, for this sample it is possible to reject null hypothesis in favor of the alternative for this sample.

Note that for these 510 decile combinations there was no positive or negative autocorrelation based on the Durbin–Watson test; the distribution of the error terms was statistically not different from normal with the Shapiro–Wilk W statistics close to one, and the error terms exhibit homoscedastic variance.

Observe that Chart 1 shows the prevalence of the individual deciles among these 510 decile combinations. They were dominated in descending order by D10, D9, D8, D7, D6, D5, D4, D1, D2, and D3. Furthermore, note that among the top ten combinations the prevalence of the individual deciles in descending order is given by D8, D9, D10, and D7.

3 year lagged New To Firm - EU

Model	Variable	OLS_Coe	OLS_Pval	OLS TRsq	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10
M_4	Intercept	(1.13)	19.690%	17.660%	-	-	-	-	-	-	-	D8	-	-
M_4	GDPCap4	0.10	2.910%	17.660%	-	-	-	-	-	-	-	D8	-	-
M_6	Intercept	(1.15)	19.400%	17.610%	-	-	-	-	-	-	-	D8	D9	-
M_6	GDPCap6	0.10	2.930%	17.610%	-	-	-	-	-	-	-	D8	D9	-
M_2	Intercept	(1.17)	19.140%	17.570%	-	-	-	-	-	-	-	-	D9	-
M_2	GDPCap2	0.10	2.950%	17.570%	-	-	-	-	-	-	-	-	D9	-
M_7	Intercept	(1.24)	18.190%	17.540%	-	-	-	-	-	-	-	D8	D9	D10
M_7	GDPCap7	0.10	2.970%	17.540%	-	-	-	-	-	-	-	D8	D9	D10
M_5	Intercept	(1.27)	17.870%	17.510%	-	-	-	-	-	-	-	D8	-	D10
M_5	GDPCap5	0.11	2.990%	17.510%	-	-	-	-	-	-	-	D8	-	D10
M_3	Intercept	(1.28)	17.750%	17.500%	-	-	-	-	-	-	-	-	D9	D10
M_3	GDPCap3	0.11	2.990%	17.500%	-	-	-	-	-	-	-	-	D9	D10
M_14	Intercept	(1.12)	20.020%	17.490%	-	-	-	-	-	-	D7	D8	D9	-
M_14	GDPCap14	0.10	2.990%	17.490%	-	-	-	-	-	-	D7	D8	D9	-
M_15	Intercept	(1.21)	18.770%	17.470%	-	-	-	-	-	-	D7	D8	D9	D10
M_15	GDPCap15	0.10	3.010%	17.470%	-	-	-	-	-	-	D7	D8	D9	D10
M_12	Intercept	(1.10)	20.560%	17.460%	-	-	-	-	-	-	D7	D8	-	-
M_12	GDPCap12	0.10	3.010%	17.460%	-	-	-	-	-	-	D7	D8	-	-
M_13	Intercept	(1.22)	18.690%	17.420%	-	-	-	-	-	-	D7	D8	-	D10
M_13	GDPCap13	0.10	3.030%	17.420%	-	-	-	-	-	-	D7	D8	-	D10
M_1023	Intercept	(1.08)	21.540%	16.960%	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10
M_1023	GDPCap1023	0.10	3.280%	16.960%	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10

TOTAL COMBINATIONS	510	510	510	510	510	510	510	510	510	510
COMBINATIONS CONTAINING DECILE:										
Number	189	187	179	197	240	248	277	337	341	356
%	37%	37%	35%	39%	47%	49%	54%	66%	67%	70%

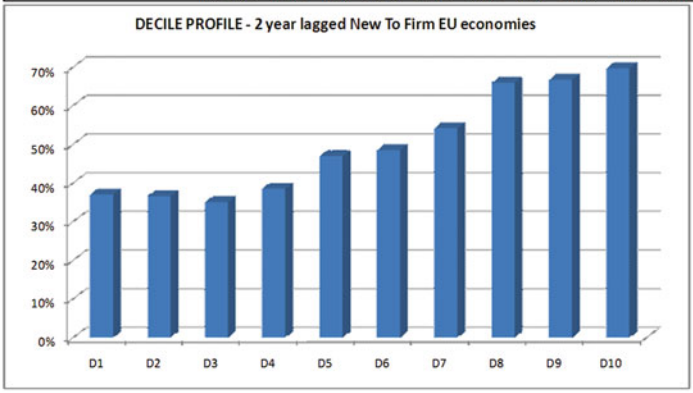

Fig. 1.3 Chart 1—Lag 3—New to firm—EU economies

1.4.4 Hypothesis 2

Regarding H2, for 168 or 33 % of these 510 decile combinations it is possible to fail to reject the null hypothesis, while for 342 or 67 % of these 510 decile combinations it is possible to reject the null in favor of the alternative. Therefore, considering all 510 decile combinations, on average the decile combinations with an explanatory power higher than that of M_1023 have a more equal distribution of income (i.e., have a lower Gini coefficient). Also, observe that all of the top 10 decile combinations ranked by R-square shown in Fig. 1.3 have Gini coefficients lower than that of M_1023.

1.5 Conclusion

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.

In the late twentieth and the beginning of the twenty-first century, numerous scholars and practitioners such as Peter Drucker have identified *knowledge* as perhaps the sixth and most important key input and output factor of economic activity. We would like to also emphasize the role and significance of *technological and economic learning* as a driver of productivity gains and an accelerator of economic growth and prosperity (Carayannis, 1993; 1994; 1998; 1999; 2000; 2001).

The e-Development towards the Knowledge Economy book attempts to address the following issues:

- How could one develop more effective and efficient mechanisms to identify, capture and disseminate critical success and failure factors and findings from ongoing e-Development interventions to enable policy-maker and practitioners to shape, evolve, and implement "smarter" e-Development strategies in real time?
- Namely, how could the most timely, appropriate, and critical e-Development priorities, objectives, and goals be integrated in a strategic context of e-Development sequence, selection, and timing choices?

In this sense, the book should be of interest and use to both public sector policy makers, private sector practitioners and policy makers, nongovernmental organizations, and academics and students of development and the role that technology can play towards catalyzing and accelerating more sustainable, equitable, and effective development interventions.

Comparing and contrasting our analysis of the development cases across developed, transitioning, and developing economies, we note a number of points partly corroborated by earlier conceptual and empirical research. The study and analysis of these, and similar cases, of e-Development towards the Knowledge Economy may provide a conceptual framework that could serve as an integrative bridge between macroeconomic, mesoeconomic, and microeconomic development ideas and themes.

The overarching goal would be to attain the right *socio-technical congruence* between e-Development intervention and the type and stage of development the targeted economy is in bearing in mind the dynamic nature of both e-Development interventions and the economies they aim to advance. In other words, one could identify optimal practices and pathways in economic development in terms of *selection, sequencing, and timing decisions* undergirding e-Development interventions in order to attain a more *functional alignment* between the social, economic, and technological dimensions of the e-Development intervention and the readiness for e-Development (e-Readiness) of the targeted economy or sectors thereof.

Functional alignment implies that an e-Development intervention is designed in such a manner, targeted at such an entry point(s) in the economy and society, and at such a time, that the optimal configuration of critical success factors (buy-in from key stakeholders, awareness, availability, affordability, and accessibility of technology, educational/health/social status of targeted social groups, and support from public and private partners in the form of public–private partnerships (PPP) among several others) will augur strongly in favor of the success of the e-Development intervention in terms of both outcomes and impacts.

References

Barney JB (1991) Firm resources and sustained competitive advantage'. J Manag 17:99–120
Carayannis EG (1993) Incrementalisme Strategique. Le Progrès Technique (no. 2), Paris, France
Carayannis EG (1994) Gestion Strategique de l'Apprentissage Technologique. Le Progrès Technique (no. 2), Paris, France
Carayannis EG (1998a) Higher order technological learning as determinant of market success in the multimedia arena: A success story, a failure, and a question to mark: Agfa/Bayer AG, enable software, and sun microsystems. Int J Technovation 18(10):639–653
Carayannis EG (1999) Knowledge transfer through technological hyperlearning in five industries. Int J Technovation 19:141–161
Carayannis EG (2000) Investigation and validation of technological learning versus market performance. Int J Technovation 20:389–400
Carayannis EG (2001) The strategic management of technological learning. learning to learn and learning to learn-how-to-learn as drivers of strategic choice and firm performance in global, technology-driven markets. CRC, Boca Raton, FL
Carayannis EG (1997) Data warehouse, electronic commerce, and technological learning: Successes and failures from government and private industry and lessons learned for 21st century electronic government. Online Journal of Internet Banking and Commerce (March)
Carayannis EG (1998b) Higher order technological learning as determinant of market success in the multimedia arena: A success story, a failure, and a question to mark: Agfa/Bayer AG, enable software, and sun microsystems. Int J Technovation 18(10):639–653
Carayannis EG (2008) Knowledge-driven creative destruction, or leveraging knowledge for competitive advantage: strategic knowledge arbitrage and serendipity as real options drivers triggered by co-opetition, co-evolution and co-specialization. Ind High Educ 22(6):343–353
Carayannis EG, Campbell DFJ (eds) (2006) Knowledge creation, diffusion and use in innovation networks and knowledge clusters: a comparative systems approach across the United States, Europe and Asia. Praeger, Westport, CT
Carayannis EG, Provance M (2007) Measuring firm innovativeness: towards a composite innovation index built on firm innovative posture, propensity and performance attributes. Int J Innovat Reg Dev 1(1):90–107
Carayannis EG, 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. J Knowl Econ 1(1):4–17
Cooper JR (1998) A multidimensional approach to the adoption of innovation. Manag Decis 36(8):493–502
Damanpour F (1991) Organizational innovation: a meta-analysis of effects of determinants and moderators. Acad Manage J 34:555–590
Drejer A (2002) Strategic management and core competencies. Quorum Books, New York, NY

Drucker PF (1985) “Entrepreneurial Strategies” innovation and entrepreneurship practice and principles. Harper & Row, New York, NY, pp 207–243
Nelson RR, Winter SG (1982) An evolutionary theory of economic change. Harvard University Press, Cambridge, MA
Penrose ET (1959) The theory of the growth of the firm. Wiley, New York, NY
Rogers EM, Shoemaker FF (1971) Communication of innovations: a cross-cultural approach. Free Press, New York, NY
Tornazky LG, Fleischer M (1990) The processes of technological innovation. DC Heath, Lexington, MA
Zaltman G et al (1973) Innovations and organizations. Wiley, New York, NY

Chapter 2
E-Development and Knowledge Economy: The Role of ICT and SME Incubation

Elias G. Carayannis

Abstract In classical economics, land, labor, and capital are the only factors of production. Knowledge, productivity, education, and intellectual capital are all regarded as exogenous factors, falling outside the system. The New Growth Theory recognizes two additional factors: technology, and the knowledge on which it is based. In today's environment, technology and knowledge are not merely additional factors of production; they have become the key factors of production. Two thematic areas are central to the analysis here: using business incubators for new venture formation, and using information and communications technology (ICT) to support and promote small- and medium-sized enterprises (SMEs). Knowledge Economy demands knowledge. Entrepreneurs need the knowledge to build a reliable infrastructure using incubators for new venture formation. New technology businesses need to move through the growth process rapidly and get their products to market before they run out of resources. Businesses need to use technology clusters to stimulate sustained innovation and growth. Educators need the knowledge to educate in ICT and e-business, attaining digital literacy for all of society, and providing the knowledge to accelerate and embrace e-commerce. Policy makers need the knowledge to accelerate and embrace e-government, providing electronic access to public services, enacting a regulatory environment conducive to the advancement of Science and Technology, and committing public policy to stimulate and assure innovation.

Keywords Conceptual framework • E-business • E-commerce • E-development • E-government • Incubators • Information and communications technology (ITC) • Innovation • Knowledge economy • Science and technology • Small and medium-sized enterprises (SMEs)

E.G. Carayannis (✉)
Department of Information Systems and Technology Management, School of Business, George Washington University, Suite 515C, Funger Hall, 2201G Street NW, Washington, DC 20052, USA
e-mail: caraye@gwu.edu

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_2, © Springer Science+Business Media New York 2014

2.1 Introduction

Technology changes the way society functions. The dramatic advances in technology over recent decades have collaterally precipitated wide sweeping and profound change to the functioning of almost every form of human exchange, the world over. What emerged in developed economies during the latter years of the twentieth century is knowledge-based economics—an evolutionary framework of social transaction that now dominates the behavior of mankind in the twenty-first century.

This paper is framed in the business management theory of knowledge economy, an operating environment rooted in technological advance—and e-development, a toolkit of practices and principles for creating and sustaining the knowledge economy.

Our examination of knowledge economy and e-development focuses on two thematic areas, both arising from, and giving rise to, the present technologic/economic revolution:

- The use of business incubators for new venture formation, and
- The use of Information and Communications Technology (ICT) to support and promote Small- and Medium-sized Enterprises (SMEs)

From the vantage of these thematic areas, we conduct a state-of-the-art survey on practices for economic development in the knowledge economy, including an in-depth investigation into the fundamental concepts and instrumental methodologies of the field, followed by a multi-dimensional analysis of 32 case studies selected for their diverse relevancies to the topical themes.

We first introduce these terminologies and concepts with definitions and backgrounds essential to their significance in the greater context of later analysis. In successive subsections we construct the environments in which these two thematic areas operate in increasingly larger spheres of significance—technology clusters, virtual incubators, technology innovation, innovation policy, and the management of science and technology—to develop a frame of reference in which the case studies are distilled and analyzed.

Assimilating and synthesizing the units of analysis, we develop thematic areas for e-development and knowledge economy interventions, in which we identify critical factors for success and failure, and encapsulate a summary of best practices for each thematic area. This is followed by an assessment of lessons learned and findings for policy and practice, from the perspective of both public and private sectors.

The paper concludes with recommendations for policy and practice of e-development in the knowledge economy and the use of incubators for venture initiation and ICT to support and promote SMEs.

2.2 The Conceptual Framework of Knowledge Economy

For countries in the vanguard of the world economy, the balance between knowledge and resources has shifted so far towards the former that knowledge has become perhaps the most important factor determining the standard of living—more than

land, than tools, than labor. Today's most technologically advanced economies are truly knowledge-based.—*World Development Report, 1999*

In classical economics, land, labor and capital are the only factors of production. Knowledge, productivity, education, and intellectual capital are all regarded as exogenous factors, falling outside the system. The New Growth Theory recognizes two additional factors: technology, and the knowledge on which it is based. In today's environment, technology and knowledge are not merely additional factors of production; they have become the key factors of production. Knowledge is 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, in turn, are drivers of economic growth. Technology raises the return on investment, which is why developed countries can sustain growth and why developing economies cannot attain growth without it. Even with unlimited labor, natural resources, and ample capital, traditional economics predicts that there are diminishing returns on investment. New Growth theorists argue that the non-rivalry and technical platform effects of new technology can lead to increasing rather than diminishing returns on technological investment.[1] Investment can make technology more valuable and vice versa. The cycle that results can raise a country's growth rate permanently—which contradicts traditional economics.

Earning monopoly rents on discoveries is important to provide incentive to invest in R&D for technological innovation. This is why protection of Intellectual Property Rights (IPR) is fundamental to growth and traditional economics sees "perfect competition" as the ideal. Enhancing human capital is critical for GDP growth, as well. To make investments in technology, a country must have sufficient human capital. Human capital is defined as the formal education, training, and on-the-job learning embodied in the workforce.

"A knowledge-driven economy is one in which the generation and exploitation of knowledge play the predominant part in the creation of wealth" (UK Department of Trade and Industry, 1998). In contrast, during the industrial era, machines replacing human labor created wealth. Nowadays, many people associate the knowledge economy with high-technology industries such as telecommunications and financial services. Actually, knowledge workers are workers who manipulate symbols rather than machines. Architects, bank workers, fashion designers, pharmaceutical researchers, teachers, and policy analysts are all examples of knowledge workers. More than 60 % of US workers are knowledge workers. For knowledge workers, *know-why* and *know-who* matters more than *know-what*. Knowledge gained by experience is as important as formal education and training—lifelong learning is vital for organizations and individuals and its intellectual capital is a firm's source of competitive advantage.

[1]The Ministry of Economic Development (2001). The Knowledge Economy: A submission to the New Zealand Government by the Minister for Information Technology's IT Advisory Group, August 1999 – What Is the Knowledge Economy? Available: http://www.med.govt.nz/pbt/infotech/knowledge_economy/knowledge_economy-04.html.

The knowledge-based economy can be characterized as fractal. It is nonlinear, unstable, and stochastic. Like chaos theory, simple algorithms iterated successively yield very complex patterns and interrelationships, as epitomized by the butterfly flapping its wings in the Amazon to trigger a hurricane over the Atlantic months later. The knowledge-based economy creates profit avalanches. Entrance is easy for small, intelligent companies, but there is no space for organic growth; the market is instantly global and a newcomer can attain dominance in 10 years. It also differentiates itself by the convergence of technologies, which removes market sector boundaries: wireless, satellite, cable, and telecom no longer belong to discrete sectors. In a mobile information society, services as well are different, impacted by the presence of Internet, virtual organization, or network transactions. ICTs are enablers of change; they release creative potential and knowledge and open up global markets and foster competition. Network transaction economies resemble the most complex network: the human brain.[2] The digital revolution can be a great equalizer, but national policies must be right to enable it. Proper training and education can make a network transaction economy, or knowledge economy, more effective and efficient: *smarter*. This elevation requires methodical enhancement of the business development environment, e.g., via business incubators. Advancement also requires enhancement of the network technology infrastructure, i.e., ICT. The state of the art is the virtual incubator, in which ICT extends and multiplies the effectiveness of business incubation at lower cost.

2.3 State-of-the-Art Survey on Practices for Economic Development in the Knowledge Economy

In this section, we delineate the fundamental concepts and instrumental methodologies of economic development in the knowledge economy. In conformance with the age of electronic information and commerce, the germane term is *e-development*. Two thematic areas are central to this paper:

- Using business incubators for new venture formation, and
- Using ICT to support and promote SMEs

We first introduce these terminologies and concepts with definitions and backgrounds essential to their significance in the greater context of later analysis. In successive subsections we construct the environments in which these two thematic

[2] Routti, Jorma (2003). Research and Innovation in Finland – Transformation into a Knowledge Economy. In *Competitiveness and the Knowledge Economy Research and Innovation Strategies: Cases of Chile and Finland*, presented at the Inter-American Development Bank, Washington, DC.

areas operate in increasingly larger spheres of significance—technology clusters, virtual incubators, technology innovation, innovation policy, and the management of science and technology—to develop a frame of reference in which 32 case studies are distilled and analyzed in multiple dimensions relevant to worldwide e-development in the knowledge economy.

2.3.1 Business Incubators for New Venture Formation in the Knowledge Economy

2.3.1.1 Business Incubators

What defines a business incubator? An incubator is an economic development tool designed to accelerate the growth and success of entrepreneurial companies. It offers an array of business support resources and services such as on-site management, marketing resources, access to appropriate rental space and flexible leases, shared basic office services and equipment, and technology support services or assistance in obtaining the financing necessary for company growth. The incubator's main goal is to produce successful firms that graduate the program financially viable and freestanding. Incubator graduates create jobs, revitalize neighborhoods, commercialize critical new technologies, and strengthen local and national economies.[3] Business incubators provide general business/corporate services, facilities and advisory services, to startups and growing companies across all sectors. Technology incubators are a specific type of business incubator, a property-based venture that provides tangible and intangible services to new technology-based firms, with the aim of helping them increase their chances of survival, generate wealth and jobs, and diffuse technology. Their objectives are economic development, technology commercialization, property venture/real estate development, and entrepreneurship. They play a visionary role in the sense that they allow governments and NGOs to demonstrate their efforts to address problems of regional development and unemployment. Figure 2.1 diagrams how different strategic objectives and competitive scopes define five archetypes of incubators.[4]

[3] National Business Incubation Association (NBIA) (2003). Principles and Best Practices – What Defines an Incubator? Available: http://www.nbia.org/resource_center/best_practices/index.php.

[4] Carayannis, Elias G. and Maximilian von Zedtwitz (2003). Architecting gloCal (global-local), real-virtual incubator networks (G-RVINs) as catalysts and accelerators of entrepreneurship in transitioning and developing economies: lessons learned and best practices from current development and business incubation practices. *Technovation*, pending publication, 2003. Elsevier Science Ltd.

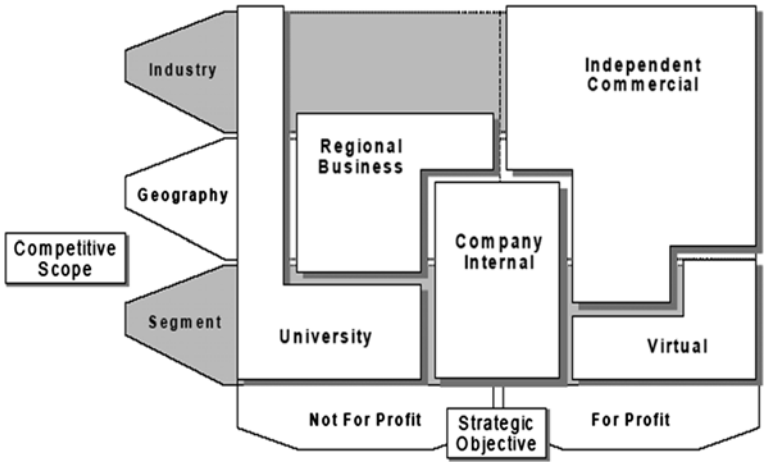

Fig. 2.1 Different strategic objectives and competitive scopes define five archetypes of incubators

2.3.1.2 International Best Practices for Incubators

The European Commission has developed a set of official recommendations for incubators distinguishing two types of audiences: the European nations and the European incubators and business centers.[5]

The recommendations to EU nations are as follows:

- Provide patient public funding support for incubator projects
- Establish clear criteria for public funding support
- Facilitate the development of incubator project networks of critical mass sufficient to attract private sector, especially in development of training and support services
- Encourage through tax incentives greater private sector funding of incubator projects, recognizing that such funding may not be forthcoming until the project is fully developed
- Carry out an impact study on incubators
- Undertake a benchmarking study to prepare a manual of good practice for anyone running or starting an incubator

[5]European Commission Directorate General XXIII and Ministry of Trade and Industry Finland (1998). Best Practices in Incubator Infrastructure and Innovation Support – Final Report: Espoo, Finland, November 19–20, 1998. Available: http://europa.eu.int/comm/enterprise/entrepreneurship/support_measures/docs/helsinki-seminar_1998_en.pdf.

- Provide finance for feasibility studies and business plan development for new companies
- Encourage educational institutions to be available to assist prospective entrepreneurs
- Facilitate Web site for incubator tenants to engage in cross-national cooperation
- Provide finance to stimulate innovation among small businesses

Recommendations to EU incubators/business centers:

- Build, maintain and utilize networks
- Develop cross-national partnerships
- Assist tenants to identify and develop partnerships
- Facilitate finance arrangements for tenants
- Commit the industrial companies
- Promote the public image of the incubator
- Demonstrate to universities and academies that the incubator operations are meritorious
- Cultivate the incubator to become a technology transfer demonstration site
- Guide the incubator to be a place of practice and educational support for professors and students
- Utilize networking to fit into local economic development processes
- Establish core services and set standards for their delivery
- Pool experience with other incubator managers to elevate standards everywhere
- Strive to increase competencies and professionalism
- Create opportunities for thinking and evaluation
- Mobilize operational teams
- Conduct internal quality assurance—measure the difference between what the incubator offers and the clients' expectations

In North America, the National Business Incubation Association (NBIA) has developed a similar set of guidelines.[6]

Recommendations to North American nations:

- First Principle: The incubator aspires to have a positive impact on its community's economic health by maximizing the success of emerging companies
- Second Principle: The incubator itself is a dynamic model of a sustainable, efficient business operation

Recommendations to North American incubators:

- Commit to the two core principles of business incubation.
- Obtain consensus on its role in the community

[6]National Business Incubation Association (NBIA) (2003). Principles and Best Practices – Two principles characterize effective business incubation. Available: http://www.nbia.org/resource_center/best_practices/index.php.

- Develop a strategic plan containing quantifiable objectives to achieve the program mission
- Structure for financial sustainability by developing and implementing a realistic business plan
- Recruit and appropriately compensate capable management
- Build an effective board of directors
- Prioritize management time to emphasize new venture assistance, proactive guidance, success, and wealth creation
- Provide facility, resources, methods, and tools that contribute to the effective delivery of business assistance
- Address the developmental needs of each company
- Integrate the incubator program and activities into the community and broader economic development goals and strategies
- Develop stakeholder support and resource networks
- Maintain a management information system and collect statistics for ongoing program evaluation, to evolve with the needs of the client startups

2.3.2 Information and Communications Technology (ICT) to Support and Promote Small- and Medium-Sized Enterprises (SMEs) in the Knowledge Economy

2.3.2.1 Overview of ICT

The ICTs cover four broad areas:

- Broadcast media, such as radio and television
- Telephone: land line, mobile/cellular/wireless/satellite, and fax
- Computers and IT Networks: WAN/LAN, Internet/World Wide Web, PCs/desktops/laptops/PDAs, e-mail, Web mail, newsgroups, and BBS (bulletin-board systems)
- Hybrid ICT Systems: telephony, text messaging, teleconferencing, portable information terminals (e.g., "i-mode" or "mobile Internet").

For the perspective of this paper, it is far more important to recognize how these devices are interrelated from a user's standpoint, rather than to understand the actual engineering behind their interconnectivity. This paper is a study of the social and economic ramifications of technology. The fusion of IT and communications into one field of ICT underscores the convergence of capabilities that are borne of the evolutionary progress of the short list, above.

Another considerable aspect to ICT is the stunning rate at which the means of information dissemination has progressed, and that this rate continues to accelerate. The terse evolution we've encapsulated here spans barely over a century, and the improvements of the latter 50 years far surpassed those of the former. And the gains of the last 15 years of computer technology arguably outstripped the 35 before. Concomitant with this acceleration in ICT is the volume of information to be

Table 2.1 Estimated time to transmit the contents of the US Library of Congress

Year	Time
1950	158,000 years
1980	661 years
1990	113 years
1992	53 days
1997	51 h

carried. It is estimated that a single copy of the New York Times contains more information than the average person of the seventieth century absorbed in a lifetime. Table 2.1 presents some statistics on the estimated time to transmit the contents of the US Library of Congress, bearing in mind that the volume of content has increased as well as the speed of transmission![7]

The salient impact of this exponentiation on business environments in the knowledge economy is paradoxical: competition has gotten stiffer, while cooperation has gotten easier.

2.3.2.2 Overview of SMEs

There is no unique definition of SME that exists and is applicable to all sectors of the economy. The European Commission and the World Bank use statistical concepts to define SMEs. For the European Commission, an SME is defined as having fewer than 250 employees, either with annual revenue not exceeding €40 million or with an annual balance sheet total not exceeding €27 million, and no more than 25 % of its capital controlled by an organization, which is not itself an SME. In EU, SMEs represent 99.8 % of all enterprises and two-thirds of all employment.[8]

In contrast, the World Bank subdivides SMEs into three groups: microenterprises, small enterprises, and medium enterprises.[9]

- Microenterprise: Ten or fewer employees, total assets not exceeding $100,000 USD, total annual sales not exceeding $100,000 USD
- Small Enterprise: Between 10 and 50 employees, total assets $100,000–$3 million USD, total annual sales $100,000–$3 million USD
- Medium Enterprise: Between 50 and 300 employees, total assets $3 million–$15 million USD, total annual sales $3 million–$15 million USD

[7] Irwin, David (2000, May). Small Business Service, Foundation for SME Development, University of Durham. Challenges for SMEs. Available: http://www.sbs.gov.uk/content/pdf/fsmed.pdf.

[8] European Space Agency (ESA) (2000). Specific for SMEs Industry Portal – SME Definition Criteria. Available: http://www.esa.int/export-ind/ESA-Article-fullArticle_par-05_1043239864433.html.

[9] World Bank Group (2000, July). Small and Medium Enterprise Initiatives. *SME Facts*, 1, 1. Available: http://wbln0018.worldbank.org/IFCExt/smepapers.nsf/0c472fee1ef0854785256a4800697d67/15639ba882dfc02785256a44005cff7c/$FILE/strat.pdf.

SMEs are characterized by their ability to react quickly to changing market conditions, which constitutes a competitive advantage. SMEs are also recognizable by their increasing shares in employment and output. SMEs lag in terms of technology adoption (at least currently), but have higher propensity for product innovation after adoption of IT. Robert-Jan Smits underscores the high priority of SMEs on political agendas since they are critical economic drivers: drivers of innovation, drivers of economic growth, and drivers of employment. However, these entities are facing critical economic challenges such as increasing competition from globalization, restrictions on access to finance, difficulties establishing networks with foreign partners, imperfect access to research results and technology transfer, speed of change in the ICT environment, uncertainty of sustainability, and lack of sources to address the information needs of small enterprises and the knowledge-based economy.[10]

2.3.2.3 ICT and Incubators

ICT and incubators afford a solution to SME challenges. ICT extends the reach and rapidity of network transactions: telephone, fax, voice mail, e-mail, and teleconferencing are technology enablers that facilitate organizational exchange so that ideas, information, knowledge, and efforts can be shared and merged with greater productivity, efficiency, and synergy and all at a lower cost. ICT also transcends geographic and political boundaries. It extends ready access to market intelligence and business resources such as industry technologies, infrastructures, and trends, competition, competitors, and emerging threats, sources of financial, technical, and managerial support, complementary producers, potential partners, and emerging opportunities, customers, potential customers, and externalities affecting those buyers, as well as suppliers and distributors, and their potential alternatives. ICT is available or can be made available to almost any environment. In developed countries, e-mail and Internet access have become ubiquitous, teleconferencing capability now has a quality level high enough to encourage real-time collaboration (RTC), replacing the need for travel in many contexts and satellite connectivity will continue to expand global access.[11]

[10] Smits, Robert-Jan and European Commission Directorate General Research – SME Unit (2000). Towards a European, European Research Area – Innovation, SMEs, and the Research Programmes of EU. Available: http://www.innovation.lv/baltdyn/presentations/Robert-Jan_Smits_Innovation,_SMEs_and_th.PDF.

[11] Kaku, Michio (1997). *Visions: How Science Will Revolutionize the 21st Century*. New York: Anchor Books.

2.3.3 Overview of Technology Clusters for Business Growth and Economic Development

2.3.3.1 Technology Clusters

A technology cluster is a critical mass of local knowledge, expertise, personnel, and resources used by firms to gain competitive advantages. Conceptually it is similar to a business incubator, but scaled larger and composed of more-established businesses. A cluster is a likely place for the incubator client to move to upon graduation.

The geographical display of clusters usually follows one of thee cluster topographic model: the hub-and-spoke model, the satellite platform industrial district model or the state-anchored district model. The hub-and-spoke model is based on one or more companies and/or central facilities as a core around which suppliers and related activities are spread. The satellite platform industrial district is a congregation of branch facilities of externally based multi-plant firms. Finally, the state-anchored districts are based on public or nonprofit organizations around which other firms and organizations clusters. The cluster formation is defined by the following attributes[12]:

- Geographic scope: natural vs. virtual clusters
- Density: dense vs. sparse
- Breadth: horizontally related industries
- Depth: vertically related industries
- Activity base: core-strategy-setting
- Growth potential: innovative vs. mature
- Innovative capacity: high vs. low
- Industrial organization: firm relationships
- Coordination: hierarchies, markets or intermediate forms

The dynamics of the cluster's performance are determined by its co-location synergy (govt. university, and firms), personal relationship, intangible (cluster culture), institutional elements, interaction logic and learning logic (know-how). In addition, we identified factors that heavily influence the creation of clusters. A Strong physical and ITC infrastructure is a baseline requirement to establish and sustain a prosperous cluster. A strong educational system is important for developing local talent and attracting outside talent. Specialized talent and training are more important than abundant labor. Universities and specialized research centers are the driving force behind innovation. Additionally, mechanisms for commercialization are essential if innovation is to translate to economic success. Finally, government can have a significant influence on the business environment both positively and negatively.

[12]Enright, Michael J. and Sun Hung Kai (2000). Survey on the Characterization of Regional Clusters. Available: http://www.urenio.org/courses/files/3/articles/Enrightsurveypdf1.pdf.

Some determinants of cluster creation are specific to the type of cluster considered, whether it is a natural, geographic cluster or a virtual cluster/network. Natural clusters are facilitated by the fact that tacit knowledge is seen as increasing in importance relative to successful innovation and because tacitness has become more important in competitive advantage under new management and organization strategies. Some wider organization change, such as closer supply chain and JIT, encourages spatial proximity as well. The increasing importance of customers—"market pull"—necessitates innovation co-location and stress is growing for external technical contacts and information sources, such as "first time" and face-to-face contact. Yet, geographic clusters can take a number of actions leading to common pitfalls. Such examples are[13]:

- Failure to communicate need to other important actors
- Cluster-killing competitive strategies of firms
- Discouraging the entrance of local rivals
- Neglecting investment in the engines of innovation; universities and research centers
- Neglecting physical infrastructure
- Government policy discouraging investment and regulation
- Focusing on narrow geographic areas
- Biases towards "high-tech" clusters (e.g., IT or biotech alone)
- Ignoring traditional strengths
- Recruiting big companies, not building competitive clusters
- Inattention to commercialization issues
- Insufficient cross-disciplinary collaboration

Conversely, some factors are more conducive of virtual clusters/networks. The increasing codification of knowledge and science, new forms of ITC, the increased dispersion of R&D, design, engineering, and technical support, both nationally and internationally, the move towards "flatter" organizations and increased managerial experiences and learning of global business management all facilitate the creation of virtual incubators.

For SMEs to engage in clusters has some clear benefits. They increase productivity and efficiency, provide efficient access to specialized inputs, employees, information, institutions, and "public goods" such as training programs and training institutions, and ease the coordination across firms. They allow for ongoing, visible performance comparisons and strong incentives to improve against local rivals, stimulate and enable innovations, and increase the ability to perceive innovation opportunities. In addition, the presence of multiple suppliers and institutions assist SMEs in knowledge creation, experimentation is made easier given locally available resources, clusters also facilitate commercialization, make opportunities for new companies and new lines of established business are more apparent and lower barriers to entry into cluster related business because of available skills, suppliers, etc. Figure 2.2 presents the constituent institutions participating in a cluster.[14]

[13] Porter, Michael E. (2001). *Clusters of Innovation: Regional Foundations of U.S. Competitiveness*. Washington, DC: Council On Competitiveness.

[14] Ibid.

Fig. 2.2 Constituent institutions participating in a cluster

2.3.4 e-Development: Virtual Incubators and Technology Cluster Networks for Business Development in the Knowledge Economy

2.3.4.1 Virtual Incubators and Clusters

ICT has advanced to the point of permitting the widespread adoption of a new kind of organizational structure: the virtual organization. Many advances in the technology enablers for virtual organization are attributable to technological standards emerging in a global network environment. Technological standards are crucial to the interoperability of networks, they make it possible to share information and communicate with a wider network, without the inefficiency of converting data formats and this enhanced sharing capacity in turn attracts more users, each representing another node on an even larger network of interconnectivity. Open standards reduce concern for consumer lock-in, ultimately broadening the market for all suppliers, which in turn improves availability to buyers.[15]

The dynamics of network interoperability are exponential. The number of connections on a network of membership networks or interactive groups is calculated by Reed's Law:

Possible connections $= 2^N - N - 1$

[N is the number of members]

[15] Shapiro, Carl and Hal R. Varian (1999). *Information Rules: A Strategic Guide to the Network Economy*. Boston, MA: Harvard Business School Press.

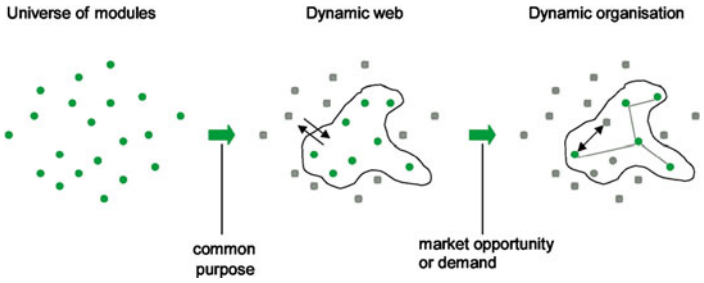

Fig. 2.3 Three layers in the virtual organization model

ICT offers a panoply of enablers for virtual organization. The virtual organization is a fluid and adaptive structure—a dynamic web, self-organizing from a community of modules, forming a new model of "organic" interconnectivity. The structure of virtual organization is reminiscent of neural net technology, based on the construct of synaptic pathways in the brain. The modern knowledge worker is analogous to a brain cell in the network of organizational intelligence. Figure 2.3 depicts three layers in the virtual organization model.[16]

The Virtual Incubator is a state-of-the-art virtual organization that provides a startup venture with global access to resources for business incubation. It is enabled by ICT and provides exponential and instantaneous connectivity to mentors, partners, managers, financing, and expertise. It provides nearly everything but the real estate. Virtual incubation services can begin as soon as the startup entity has access to the Internet.

2.3.5 Fundamental Concepts of Innovation and the Role of SMEs for Innovation in the Knowledge Economy

2.3.5.1 Concepts of Innovation

What is Innovation? Innovation is the specific instrument of entrepreneurship. There is no such thing as a "resource" until man finds a use for something in nature and endows it with economic value. Without innovation, crude oil seeping out of the ground was a nuisance, so was penicillin mold on food and books were not available

[16] Saabeel, W., T.M. Verduijn, L. Hagdorn, and K. Kumar (2002). A Model of Virtual Organisation: A Structure and Process Perspective. *Electronic Journal of Organizational Virtualness* 1, 2002. Available: http://www.virtual-organization.net/files/articles/Saabeel-Verduijn-2002.pdf.

Fig. 2.4 Innovation system model based on input and factors

to permit universal education. Innovation does not require high-tech (e.g., insurance, advertising, installment buying). Innovation is social and economic more than technical; it changes economics from supply terms to demand terms, increasing the value and satisfaction obtained from resources by the consumer. Innovation is the cultivation of knowledge, materials, and methods into economic practice for improved competitive advantage. It is the transformation of an invention generated by scientific activity into a socially usable product.[17] An innovation system model based on input and factors appears at Fig. 2.4.[18]

[17]Drucker, Peter F. (1993). *Innovation and Entrepreneurship*. New York: Harper & Row, Publishers, Inc.

[18]Carayannis, Elias G. (2003, June). Competitiveness, Productivity and Innovation. In *Management of International Science and Technology*, presented at the School of Business and Public Management, GWU, Washington, DC.

Systematic innovation is a purposeful and organized search for changes and the systematic analysis of the opportunities such change might offer for economic and social improvement. Invention alone is not innovation: to qualify as innovation, an invention must be brought to commercial acceptance—great ideas left on the shelf benefit none and great inventions that nobody buys benefit none. Invention used to be a mysterious "flash of genius," but by World War I, it had become systematic research.[19] Innovation is market actualization.

2.3.5.2 Innovation and SMEs

Factors such as organizational culture, entrepreneurship, flexibility, creativity, economic pressures, competition, reactivity, and survival position SMEs as drivers of innovation. In many fields, SMEs provide the channels along which new technologies develop. In sectors such as biotechnology and information technology, relatively small numbers of new, technology-based firms (NTBFs) are key suppliers of new technologies. The ability to exploit new technologies and respond quickly to changing market needs give SMEs a pivotal role in economic success: introducing new products, enhancing existing products, developing technology, and being willing to collaborate.

2.3.6 Overview of Innovation Policy for e-Development in the Knowledge Economy

2.3.6.1 Innovation Policy

The concept of "innovation system" is now accepted as key to national competitiveness. It evolves in an environment of flux and continual change (global markets and knowledge economy) and generates the need for evaluating trends in national innovation policies by analyzing and benchmarking and disseminating good practice and focusing on key areas, such as intellectual property rights (IPR), innovation financing (R&D intensity), or the creation of more new technology-based enterprise (incubation). Governments, drafting national policies, also became involved in the design of innovation policy. Governments formulate and enact the regulatory environment: fields of R&D are steered by law, political culture, central planning, and some avenues of research may be mandated, others are banned, and IPR protections are guaranteed, neglected, or dismissed. Governments stage the economic climate: R&D can be directly funded or subsidized from national budgets, tax incentives, and other inducements can attract private investments.[20]

---

[19] Drucker, op. cit.

[20] Development Gateway (2003). Innovation Policy. Available: http://www.developmentgateway.org/node/130667/browser/?keyword%5flist=137331&country%5flist=0.

Innovation is stimulated by Government, University, and Industry (GUI) alliances for collaborative R&D. The government usually provides about 50 % of the funds and/or facilities, universities provide scientific expertise and researchers on fellowship, and the industry provides balance of funding, practical expertise, and market forecasts. Under these alliances, companies use co-opetition as the term for competitors collaborating under nondisclosure agreements to enlarge and enhance market opportunity under pre-competitive conditions. GUIs rely on technology transfer, researchers working for government or university labs are permitted or even encouraged to file for IPR protections in conjunction with their R&D contributions, and personally benefit financially from any subsequent commercialization. The Cooperative Research and Development Agreement (CRADA) is an example of US GUI agreement form for controlled knowledge sharing and technology transfer.[21]

We notice a significant shift in trend over the past couple decades. During the 1980s and 1990s, it was estimated that the lag time between government R&D spending and resultant benefit to GDP growth was 15–20 years. In the twenty-first century, it is apparent that the economic payback is quicker, and the level of investment is more cost effective.[22] This is a phenomenon of the knowledge economy, enabled by ICT and Business Incubators. Incentives for productive innovation depend on enforceable protections of Intellectual Property Rights (IPR) such as patents (lasts 14–20 years), trademarks ™ (lasts in perpetuity), copyright © (lasts for life of author plus 90 years), or trade Secret (lasts until the secret is discovered—not stolen; there are legal protections against theft of trade secrets).

2.3.6.2 Leaders in Research Intensity

The following tables and graphics point to some of the leaders in research intensity and innovation. One method to measure research intensity is Gross Domestic Expenditure on R&D (GERD) as a percentage of GDP. Table 2.2 presents a quick summary of recent data. Another way to measure R&D intensity is the percentage of workforce engaged as researchers. Table 2.2 also shows comparatives of this metric. Figure 2.5 charts the R&D intensity by nation for the global leaders, based on the most recently available data: 2002 for the USA; 2001 for D, E, F; 2000 for I, NL, FIN, UK, EU-15, JP; 1999 for all others.

[21] Stewart, McDonald R. and John J. Wetter (2002, January). International Science and Technology Policy. In *Management of International Science and Technology*, presented at the School of Business and Public Management, GWU, Washington, DC.

[22] Milbergs, Egils. (2002, February). Technology policy, prosperity and security from 1980 to the 21st century. In *Program in management of science, technology and innovation*, presented at the School of Business and Public Management, GWU, Washington, DC.

Table 2.2 Leaders in research intensity (2002) [national average, including all levels of technology]

	R&D Spending % of GDP[a]	Researcher % of Workforce[b]
EU	1.94 % mean[c]	2.5 %
USA	2.80 %	6.7 %
Japan	2.98 %	6.0 %

[a]European Commission Research (2003). Red Alert for European Research: Speeding Up Knowledge Investments is More Than Urgent. *Science and Technology Indicators 2003: The Latest Data on Europe's R&D Performance, 11*. Available: http://europa.eu.int/comm/research/press/2003/pdf/indicators2003/11-investment_en.pdf [2003, June 25].
[b]Smits, op. cit.
[c]EU range: Greece 0.67 %–Sweden 3.65 %

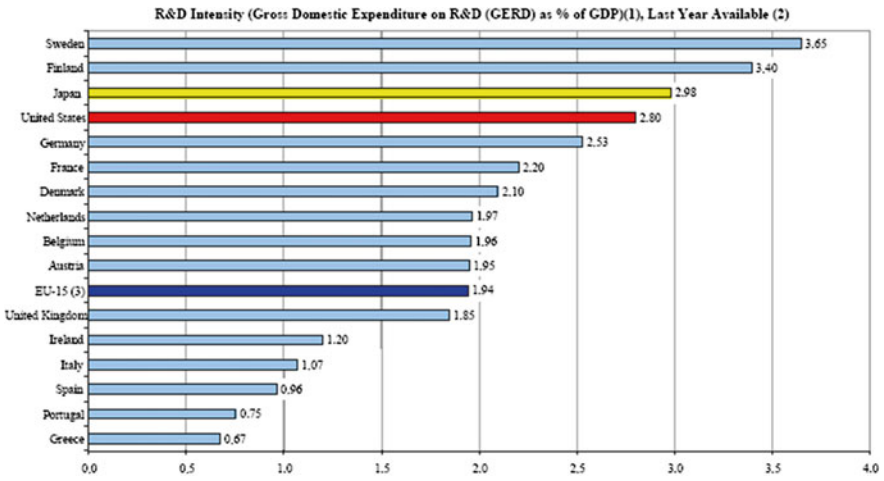

Fig. 2.5 R&D intensity by nation. European Commission Research, op. cit.

2.3.6.3 Investments in Knowledge

The OECD considers investments in knowledge to be a valuable composite metric for sustainability in the knowledge economy, counting expenditures in R&D, software, and higher education. Figure 2.6 plots total investments in knowledge as a percentage of GDP for the world's leading nations, aggregated for the period 1991–1998. The chart also shows the sum for each country at the outset of the period to suggest a trend for each.[23]

[23]Organisation for Economic Co-Operation and Development (OECD) (2003). Report on Investments in Science and Technology. Available: http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-0-nodirectorate-no-12-35175-0,00.html.

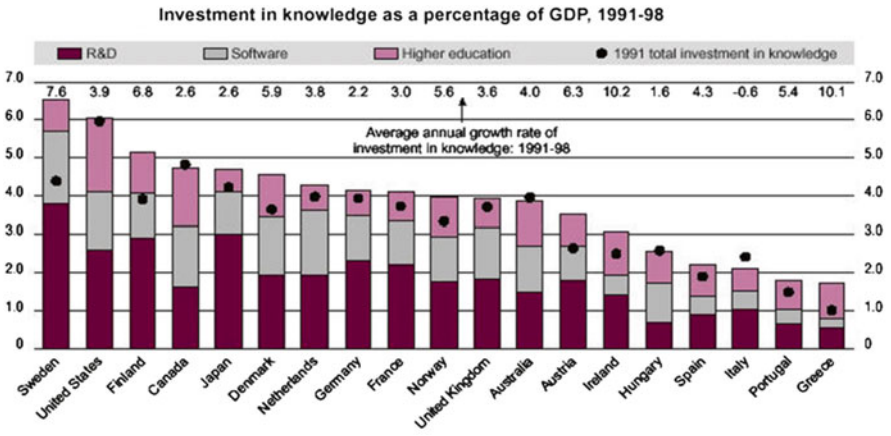

Fig. 2.6 Investment in knowledge as percentage of GDP 1991–1998

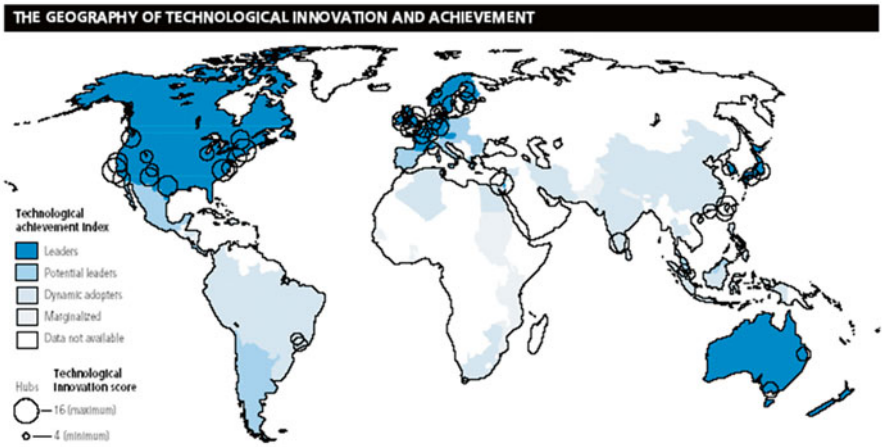

Fig. 2.7 The geography of technological innovation and achievement. United Nations Development Programme (UNDP) (2003). Today's technological transformations – creating the network age. *Human Development Report 2001: Making new technologies work for human development, Chapter 2 (p. 45).* Available: http://hdr.undp.org/reports/global/2001/en/pdf/chaptertwo.pdf [2003, June 23]

2.3.6.4 Global Hubs of Technological Innovation

Figure 2.7 maps the geography of technical innovation and achievement, rating global regions and hubs according to indices for technological achievement and technological innovation.

2.3.7 Conceptual Framework of Science and Technology

Science and Technology

Prominent thinkers have defined science in different ways. According to Sir Karl Popper, science is the systematic search for truth by testing and invalidating all unsatisfactory attempts to define it.[24] Truth is the prevailing consensus among knowledgeable researchers and science is the evolutionary process whereby human knowledge advances.[25] Conversely, technology is defined as "a design for instrumental action that reduces the uncertainty in the cause–effect relationships involved in achieving a desired outcome and should be conceived of as a process rather than a product… A system… by which society satisfies its needs and wants or knowledge of how to do things."[26] Sahal tells us that technology is a pattern of artifact design to chart the course of further innovations in a self-organizing system of stepwise improvements.[27]

In brief, technology is the evolutionary culmination of humanity's learning and fabrication skills, toward manipulation of our environment. Science is what we know and how we know it; technology is how we apply that knowledge to improve the human condition.

In many cases, the advance of science goes hand in hand with the advance of technology. Together science and technology (S&T) account for the progress and prosperity attained at an accelerating rate since the beginnings of the industrial revolution. Scientific research and development (R&D) explores the avenues for technological innovation, technology is both a driver and an outcome of economic commerce. Technological progress creates the jobs of tomorrow, but scientific research creates the jobs of the day after tomorrow. Both science and technology are knowledge, and knowledge is experience, know-how. Hence the goal of R&D is to develop knowledge faster, better, and cheaper!

2.3.7.1 Instrumental Methodologies in the Management of Science, Technology, and Innovation for e-Development in the Knowledge Economy

Creativity, Innovation, and Competitiveness

Creativity is a private process operating at the individual or micro level; it consists in seeing the things everyone else is, but thinking about them differently. Innovation can be viewed as the successful diffusion of creativity into society, mostly at the

[24] Miller, David W. (Ed.). (1985). Popper selections. Princeton, NJ: Princeton University Press.

[25] Kuhn, Thomas S. (1996). The structure of scientific revolutions (3rd ed.). Chicago: The University of Chicago Press.

[26] Carayannis, Elias G. (1999, June). Key concepts defined: Technology management, productivity, competitiveness, innovation, and intellectual property rights. In *Management of International Science and Technology*, presented at the School of Business and Public Management, GWU, Washington, DC.

[27] Sahal, D. (1985). Patterns of technological innovation. In M. J. C. Martin (Ed.), *Managing innovation and entrepreneurship in technology based firms* (p. 38). New York: John Wiley & Sons, Inc.

organizational or meso level. Finally, competitiveness is the capacity of society to apply innovation to achieve superior outputs and outcomes, mostly at the national or macro level—in particular to add value, while using the same or lower amounts of inputs.[28]

Creativity, Innovation, and Competitiveness can be modeled as a double helix, akin to nature's fundamental scaffold and evolutionary competence. One strand represents the flow and record of creativity, the other that of competitiveness. The value-adding chain of creativity, invention, innovation, productivity and competitiveness links both strands. This chain catalyzes learning and meta-learning to do things better, cheaper, and faster at the micro, meso, and macro level. The gains are reflected in higher standards of living, an increase in the number of competitive firms, more robust economies and the accelerated and more sustainable development trends.[29]

The Wheel of Innovation, Productivity, and Competitiveness

Figure 2.8 shows a model of the interrelationships among innovation, productivity, and competitiveness, as pertain to the depth of internal and external factors of the concentric spheres, one for each level: firm, industry, national, and transnational.

Drivers, Mechanisms, and Outcomes of Innovation

Figure 2.9 illustrates a closed innovation system, in which a research facility operates in an insular capacity, attempting to self-supply all its own knowledge capital. Figure 2.10 revises the model to the open innovation paradigm, wherein knowledge is shared among research entities to catalyze creativity and leverage innovation to mutual benefit.

Technology Creation, Transfer and Commercialization

Figure 2.11 charts the structure and flow of technology creation, transfer and commercialization, positioning the hierarchy of actions and platforms of commercialization of technology, customer focus, technology stock, acquisition of technology, and competence of personnel, against the cross controls of IP protection and management focus.

---

[28]Carayannis, Elias G. And Edgar Gonzalez (2003). Creativity and Innovation=Competitiveness? When, How, and Why. *International Handbook on Innovation, Chapter 3*, pending publication, 2003. Elsevier Science Ltd.

[29]Ibid.

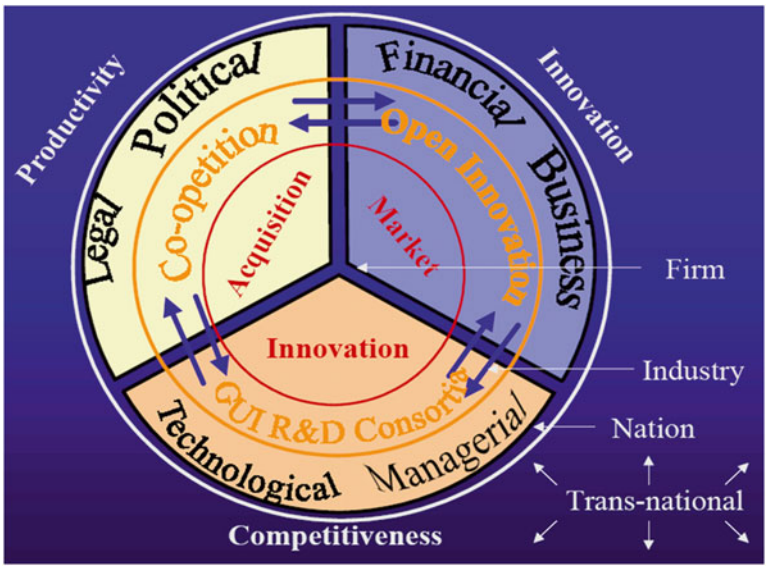

Fig. 2.8 The wheel of innovation, productivity, and competitiveness. Carayannis, Elias G. (2003, June). Competitiveness, Productivity, and Innovation, op. cit.

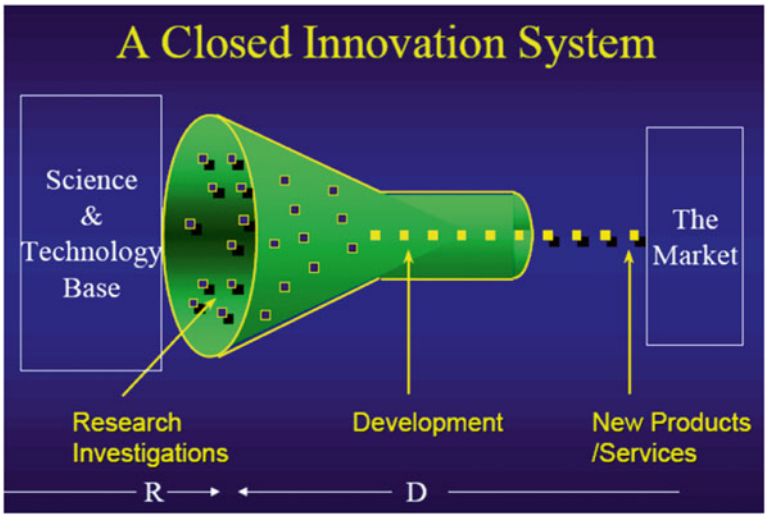

Fig. 2.9 A closed innovation system. Chesbrough, Henry (2001). Open Innovation: A New Paradigm for Managing Technology. In *New Business Strategies for R&D*, presented to OECD Conference [2001, October 22]

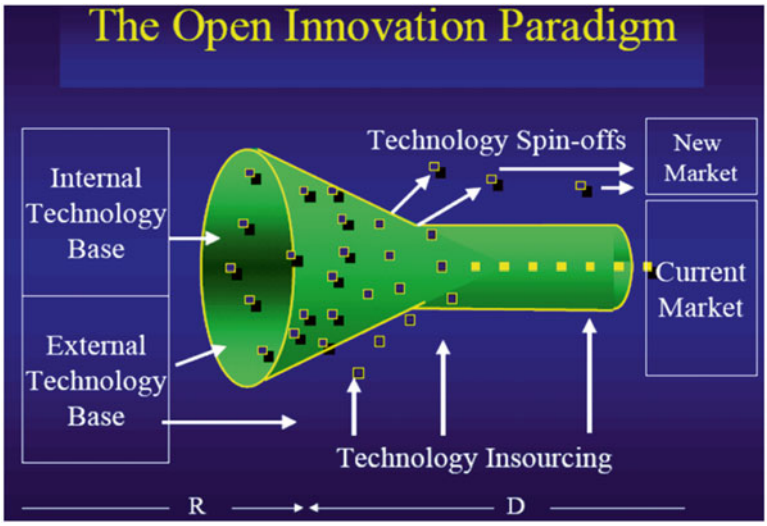

Fig. 2.10 The open innovation paradigm. Ibid

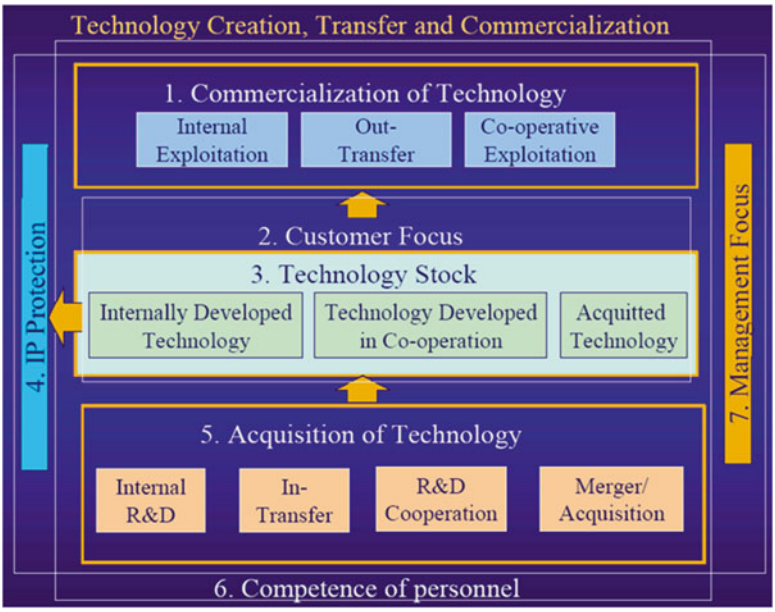

Fig. 2.11 Technology creation, transfer, and commercialization. Carayannis, Elias G. (2003, June). Competitiveness, Productivity, and Innovation, op. cit.

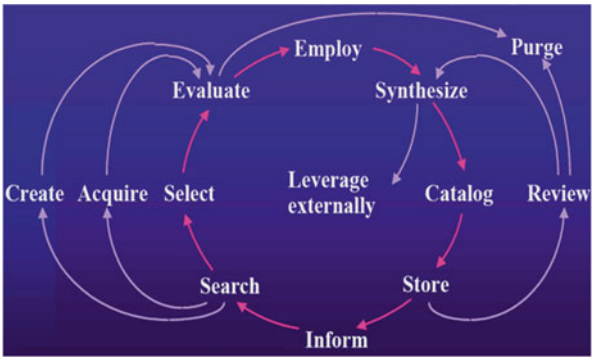

Fig. 2.12 The continuous process of knowledge capture

2.3.8 The Impact of Discontinuous and Disruptive Innovations on e-Development and Knowledge Economy

2.3.8.1 Discontinuous and Disruptive Innovations

Knowledge management is the systematic, explicit and deliberate building, renewal, and application of knowledge to maximize an enterprise's related effectiveness and returns from its knowledge assets. It is about managing information *and* managing people. Management of innovation can benefit from systematic approach to knowledge management by distinguishing what information is most relevant and significant to the management of innovation, especially since some knowledge is explicit, but some is tacit and therefore more difficult to record and comprehend.[30]

Knowledge capture is a continuous process wherein learning and information are derived through numerous channels, filtered, adjusted, recorded, assimilated, and deployed (or rejected) by the actors within the organizational context. This process is depicted at Fig. 2.12.[31]

Meta-cognition is to think about thinking, meta-learning is to learn about learning, and meta-knowledge is to know about knowing. The progression of knowledge capture, at the level of the individual or the organization is from data to information to knowledge to wisdom to intuition. In the Organizational Cognition Spiral (OCS), modeled at Fig. 2.13, K is knowledge and M is meta-knowledge. The dimensions are assumed to be at two levels representing the presence and absence of (meta)

[30]Carayannis, Elias G., Edgar Gonzales, and John J. Wetter (2003). The Nature and Dynamics of Discontinuous and Disruptive Innovations from a Learning and Knowledge Management Perspective, *Chapter 7*, pending publication, 2003. Elsevier Science Ltd.

[31]Arthur D. Little Inc. (2003). The Value Necklace: Acquiring knowledge - Capturing knowledge is a continuous process. *Changeintelecom.ppt*. Cambridge, England: Author.

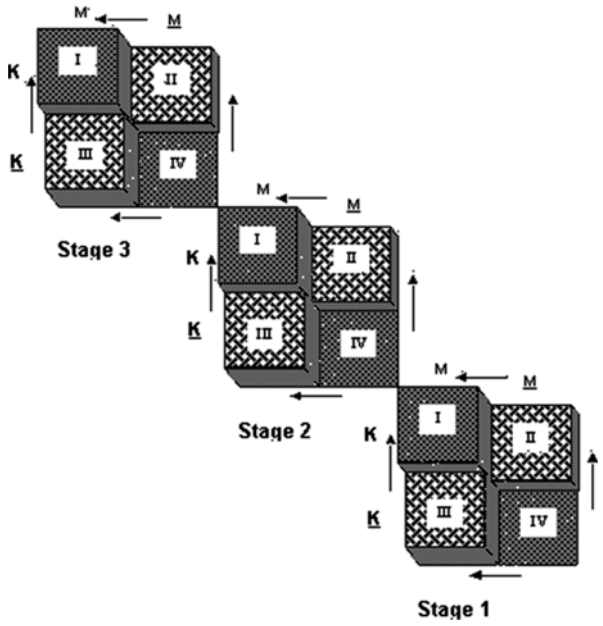

Fig. 2.13 The organizational cognition spiral (OCS)

knowledge. The levels of the two dimensions are thus represented as K and *K*, and M and *M*. These two levels of the two dimensions result in four knowledge states:

1. K, M (awareness of awareness)
2. K, *M* (ignorance of awareness)
3. *K*, M (awareness of ignorance)
4. *K*, *M* (ignorance of ignorance)

The successive stages (1, 2, 3) denote cumulatively higher levels of knowledge and meta-knowledge.[32]

2.3.9 Three Dimensions of Analysis of e-Development in the Knowledge Economy

This section introduces the analytic framework to be applied to a diverse selection of case studies, grounded in the fundamental concepts and instrumental methodologies of e-development and knowledge economy as delineated above, and respective

[32]Carayannis, Gonzales & Wetter, op. cit.

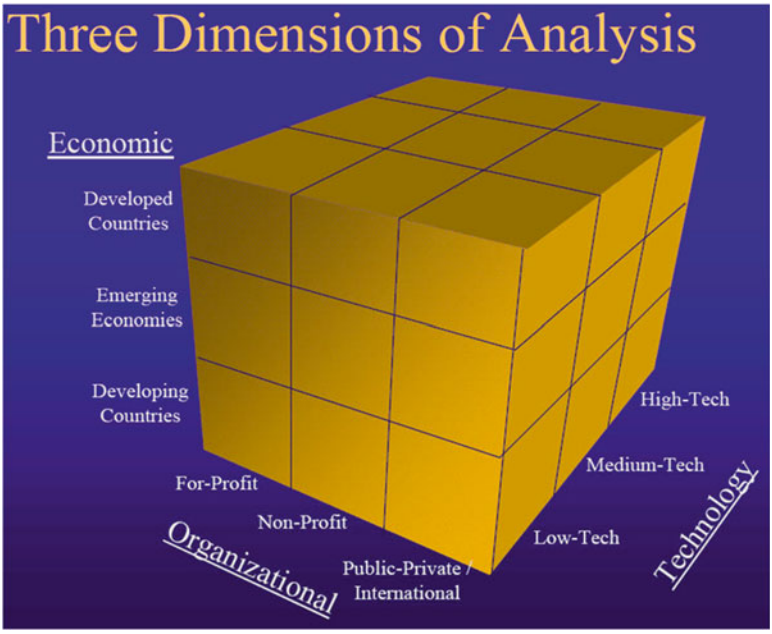

Fig. 2.14 Three dimensions of analysis

of the two thematic areas of this paper: using business incubators for new venture formation, and using ICT to support and promote SMEs.

Each case study is coded in three dimensions for evaluation: economic level, organizational level, and technology level, and each level is subdivided into three sublevels. Tabulation of these analytic dimensions yields 27 points of conjunctional cells, as illustrated in Fig. 2.14. At least one case study has been selected to embody each conjunction in the matrices. Some cases, by their scope, span multiple cells. Some cells contain multiple case studies. A total of 32 case studies are summarized and analyzed in this state-of-the-art survey, to afford substantive information in each analytic dimension.

2.3.9.1 Economic Level: Developing Countries, Emerging Economies, Developed Countries

The economic level is further broken down into developed countries, developing countries and emerging economies, as special case of developing countries. In developed countries, quality of life in rural areas is comparable to that in the urban areas. Developed countries have reached a stage of economic development characterized by the growth of industrialization, the amount of money made by the population (national income) is enough to pay for schools, hospitals and other services; and

their population growth is usually slower than in developing countries. In simple terms, the World Bank defines them as follows[33]:

> **Developed countries (industrial countries, industrially advanced countries)** High-income countries, in which most people have a high standard of living. Sometimes also defined as countries with a large stock of physical capital, in which most people undertake highly specialized activities. According to the World Bank classification, these include all high-income economies except Hong Kong (China), Israel, Kuwait, Singapore, and the United Arab Emirates. Depending on who defines them, developed countries may also include middle-income countries with transition economies, because these countries are highly industrialized. Developed countries contain about 15 % of the world's population. They are also sometimes referred to as "the North."

Developing countries comprise low- and middle-income countries where most people have lower standard of living with access to fewer goods and services than most people in high-income countries. Currently about 125 developing countries with populations over one million; in 1998, their total population was more than 5.0 billion. Developing countries are broadly split into two categories, the middle-income and the low-income groups. According to 2002 statistics, the GNP per capita of middle-income countries ranged from $755 to $9,266; low-income countries, also referred to as Least Developed Countries (LCDs), had a GNP per capita below $755.[34]

Emerging economies are the most economically progressed of developing countries. In terms of GNP per capita, they correspond to the medium-low and medium-high country groups but are characterized by a regulated and functioning securities exchange, or in the process of developing one, and the fact that shares traded on the stock exchanges must be available for purchase by foreign investors, even if subject to certain restrictions.[35]

2.3.9.2 Organizational Level: For-profit, Nonprofit, Public–Private/International

At the organizational level, we focused on for-profit, nonprofit, and public–private/international entities.

A for-profit entity is any organization whose primary objective is to have revenues exceed expenses and return the remainder (profit) to its shareholders. These could be private or public enterprise, business, firm, proprietorship, partnership, corporation, or other form of organization having emphasis on the financial performance metrics of operations. In the event of dissolution, the assets owned by a for-profit entity are

---

[33] Soubbotina, T. with K. A. Sheran (2000). The World Bank Group – Beyond Economic Growth: The Challenges of Global Development. Available: http://www.worldbank.org/depweb/beyond/global/glossary.html.

[34] The World Bank Group. Learning and Knowledge: For Schools – Glossary. Available: http://www.worldbank.org/html/schools/glossary.htm.

[35] Kovalskaya, S., I. Tchekounaeva and E. Zakhriapa (2002). *Emerging Markets: An Introduction*. Corporate Finance – Master Classes. The International College of Economics and Finance. Higher School of Economics. Russia. Available: http://www.hse.ru/icef/masterclass/emerging_markets.ppt.

Table 2.3 Constituents of public–private/international organizational level

Governments, governmental agencies, and governmental alliances at all levels	Publicly subsidized institutions for education or research	Large Nongovernmental Organizations (NGOs)	Alliances and consortia for research and development, collaborating
International (e.g., UN, EU, NATO, CIS)	Universities, colleges	International in scope, crossing technical, economic, and political boundaries	Government, as described in the first column
National (e.g., countries)	Hospitals, laboratories	Having far-reaching influence in economic development, e.g., World Bank, IADB, OECD, WTO	University, including nonprofit research hospitals and labs
Local (e.g., states, provinces, counties, districts)	Think tanks, skunk works		Industry, representing for-profit businesses
Municipal (e.g., cities, towns, villages)			

distributed to creditors and individual owners. This type of organization is typically taxed by governmental authorities.

Nonprofit entities, also including not-for-profit and non-for-profit, are an association or organization of persons banded together for a specific purpose. Under US Code, the association must have a written document showing its creation, with at least two persons attesting. The definition of an association can vary under state law.[36] The primary purposes of operation are exclusively for religious, charitable, scientific, literary, cultural, educational, recreational or other nonprofit pursuits. This definition also comprises some nongovernmental organizations (NGOs) that are local in scope or serving small-scale transnational interests, e.g., professional associations, regional development authorities. Nonprofit organizations can be privately held, but they should not distribute profit to individual members in any form. In addition, no part of the assets, income, or earnings of the entity is to benefit any individual or member. In the event of dissolution, the assets owned by such association, corporation, or other entity are distributed to another association, corporation, or other nonprofit entity. Nonprofit organizations may qualify for tax-exempt status.[37]

The third subset of the organizational level of analysis we broadly refer to as public–private/international. This encompasses government, governmental agencies, and governmental alliances at all levels, publicly subsidized institutions for education or research, large NGOs, and alliances and consortia for research and development, that are collaborating. Some illustrations and examples are provided in Table 2.3, above.

[36]Internal Revenue Service. Charities & Non-profits. Available: http://www.irs.gov/charities/article/0,,id=96120,00.html.

[37]Neal S. Blaisdell Center & Waikiki Shell (2003). City & County of Honolulu – Department of Enterprise Services. http://www.blaisdellcenter.com/techrental/NON_ADM_Non_Prof_Rates.pdf.

2.3.9.3 Technology Level: Low-Tech, Medium-Tech, High-Tech

Ultimately, we refined the analysis at the technology level, differentiating low, medium, and high tech.[38]

The entities qualifying for one of the following four criteria were considered high-tech:

1. Makers and creators of new technology, whether in the form of products, communications, or services
2. Engaged in the development, market deployment, or adoption of innovation and emerging technologies, such as biotech (e.g., pharmacology, genomics, bioinformatics, pharmacogenetics), IT/ICT (e.g., Wi-Fi, i-mode, robotics, neural networks, photonics) or materials engineering (e.g., ceramics, polymers, semiconductors, composites)
3. Devoting the bulk of assets to R&D, value lies almost entirely in the future
4. R&D intensity: Industry spending more than 4 % of turnover (e.g., ICT or pharmaceutical)

To qualify as medium-tech the organizations under consideration met one of three criteria:

1. Manufacturers and producers of existing technology, whether products, communications, or services
2. Engaged in the fabrication, process improvement, or incremental innovation of established technologies
3. R&D intensity: Industry spending between 1 and 4 % of turnover (e.g., vehicles and chemicals)

Finally, entities qualifying as low-tech were matched on of three criteria:

1. Producers and harvesters of mature technology
2. Engaged in the replication and maintenance of mature technologies
3. R&D intensity: Industry spending less than 1 % (e.g., such as textiles or food)

2.3.10 Real Practices in e-Development and Knowledge Economy: Case Studies

Not all best practices are real and not all real practices are best—Carayannis

In this section, we present 32 case studies, with at least one selected to embody each of the 27 possible conjunctional cells of analysis based on the criteria defined in our three-dimensional model. Some cases, by their scope, span multiple cells. Some cells contain multiple case studies.

[38] Smith, Keith (2000). Innovation Indicators and the Knowledge Economy: Concepts, Results and Policy Challenges. In Paper presented to Conference on Innovation and Enterprise Creation: statistics and indicators, Sophia Antipolis, France, 23–24 November 2000. Available: http://pwp.netcabo.pt/ana.moutinho/Docs/InnovationIndicators.doc.

Table 2.4 Constituents of public–private/international organizational level

Entrepreneur quality	*Resource-based capability*	*Competitive strategy*	*Financial consideration*
Enthusiasm	Input sourcing	Customization	Liquidity of investment
Capacity for work and sustained intense effort	Managerial and marketing	Innovation	Years to expected return
Creativity	Capabilities	Quality	Subsequent investment
Familiarity with target market	Technical capability	Cost	First round only
Competence	*Product characteristics*	*Market characteristics*	*Performance measures*
Desire for success	Uniqueness	Established distribution channels	Sales
Courage	Protection of product	Untapped potential	Market share
Leadership	Development abandoned	Market growth rate	Marketing cost
Ability to evaluate and react to risk well	Developed to prototype	Stimulation of existing market	Production cost
Attention to detail	Market acceptance	Familiarity with industry structure	General and administrative cost
Ability to articulate		Early-stage competition	ROI
Track record		New market/segment creation	Profits

The cases are subdivided and grouped by thematic area. The first 15 cases pertain primarily to the theme of using business incubators for new venture formation, followed by 17 cases that pertain primarily to the theme of using ICT to support and promote SMEs. We found these two themes to be so interdependent that there is considerable overlap within many individual cases, but in preparing the case summaries, we have attempted to focus on the theme for which each case study was coded.

2.3.11 Case Studies in the Use of Business Incubators for New Venture Formation

Real Practices—Case 1	Economic level:	Developed and developing countries	Business Incubators for New Venture Formation
Venture Capitalist Survey on Success Factors[39]	Organizational level:	For-profit	
	Technology level:	High-tech	

Kakati conducted a survey with 27 venture capitalists in order to find out which were the determinants of viability and achievement of new ventures. The venture capitalists, having experience with multiple high-tech ventures, both successes and failures, in both developed western nations and India/Southeast Asia, were asked to rank 25 predetermined criteria covering seven dimensions, as shown in Table 2.4.

[39] Kakati, M. (2003). Success criteria in high-tech new ventures. *Technovation*, 23 (2003) 447–457. Elsevier Science Ltd.

The survey identified that the specific factors accounting for the majority of venture successes were:

1. Ability to evaluate and react to risk well
2. Protection of product
3. Stimulation of existing market

And the ones accounting for the majority of venture failures:

1. Incapability risk: principally marketing, input sourcing, and managerial
2. Inexperience risk: familiarity with target market and relevant track record
3. Product risk: Uniqueness of product/service relative to competitors (differentiation), product protection, untapped market potential

Real Practices—Case 2	Economic level:	Developing countries	Business
UNECE Promotes Development in Eastern Europe[40]	Organizational level:	Public–private/international	Incubators for New Venture Formation
	Technology level:	Medium-tech	

The United Nations Economic Commission (UNECE) established the Working Party on Industry and Enterprise Development for Europe in 2000. It serves specifically Eastern Europe, the Baltic States, and CIS. The priority purposes agreed upon at their summit are:

- To build bridges between East and West;
- To promote enterprise development and capacity building;
- To advocate public–private partnership and private sector involvement in economic development;
- To introduce best practices from UNECE networks;
- To promote electronic techniques for business communications and practices in countries in transition; and
- To bring together decision-makers from business and government.

Real Practices—Case 3	Economic level:	Emerging economy	Business Incubators for New Venture Formation
Business Incubator for Women Enterprise Center in Jordan[41]	Organizational level:	For-profit	
	Technology level:	Low-tech	

Although incubators and incubation of small enterprises is a new idea worldwide, Jordan tested and applied this idea in two different cases. One of them is the "Business Incubator for Women Enterprise Center, which was considered to be a

[40]United Nations Economic Commission for Europe (UNECE) (2001). UNECE Guidelines on Best Practice in Business Incubation (2nd Ed.). *Publication ECE/Trade/265*. Available: http://www.unece.org/trade/entdev/tmp/ecetrade265.pdf.

[41]Rawabdeh, Ibrahim A. and Brent Strong (2003). Developing Technical Entrepreneurship In Less Developed Countries (A Case Study of Jordan). Brigham Young University, College of Engineering and Technology. Available: http://class.et.byu.edu/mfg210/Papers/Dev%20Tech%20Entre%20Jordan%20rev2.doc.

nonprofit incubator. The Business Incubator for Women Enterprise Center is considered a distinctive pioneer experience in the Middle East, and it is the first of its kind in Jordan. It was established in 1996. This incubator faced difficulties of limited space, but it still provided a reasonably complete package of services necessary for new enterprises. As the actual working space is one of the principle features of an incubator, and one of the main problems for the Business Incubator for Women Enterprise Center, the management of the incubator has started to implement another pioneering idea. This new method of supporting small enterprises is called "incubator without walls." It offers the same services and technical consultation but is given to enterprises on their field sites. At the same time, the present incubator will form the center for development of the enterprises of the open incubator."

Real Practices—Case 4	Economic level:	Emerging economy	Business Incubators
Jordan Technology Group[42]	Organizational level:	For-profit	for New Venture
	Technology level:	Medium-tech	Formation

The second case Jordan applied was the Jordan Technology Group (JTG), a for-profit incubator. "The Jordan Technology Group is an established venture capital company that invests in technology-based enterprises in Jordan and the region, with over 10 years of investing and incubating experience. The JTG incubator focuses on the information technology (IT) industry and related technologies that have high potential in Jordan and regional markets. JTGs' investments include working with entrepreneurs at early stages to develop high potential technology and to create the company to produce and market the products. JTG is an experienced and reliable venture capital partner providing funding and advice to create value and get effective results for the companies in which it invests and for investors whose funds it manages. While the program has been relatively successful (13 companies have successfully been launched over a period of 10 years), it is under-capitalized and it is of limited impact in terms of the total needs of the IT sector."

Real Practices—Case 5	Economic level:	Emerging economy	Business Incubators
Hsinchu Industrial Park,	Organizational level:	Non-profit	for New Venture
Taiwan[43]	Technology level:	Medium-tech	Formation

Although tackling the causes of the talent drain will take time for most countries, Taiwan is an exception. "The Hsinchu Science-Based Industrial Park is a key attraction: Silicon Valley returnees started more than half of the companies there, and it now accounts for roughly 10 % of Taiwan's gross national product."

In the 1990s, roughly 650,000 people from emerging markets migrated to the USA on professional-employment visas. Over 40 % of foreign-born adults in the USA have at least some college education, making the USA the epicenter of global talent drain. Foreign-born workers now make up 20 % of all employees in the US

[42] Ibid.

[43] Devan, Janamitra and Parth S. Tewari, (2003). When the Best Brains Go Abroad. *IEEE Spectrum*. Available: http://www.spectrum.ieee.org/careers/careerstemplate.jsp?ArticleId=n100101.

information technology sector and globally, approximately a third of R&D professionals of developing countries have left them to work in the USA, EU, or Japan. Many S&T expatriates have returned to Taiwan, attracted by their nation's long commitment to building a market-oriented economy, coupled with initiatives such as the creation of a venture capital industry and investments in research and education—has prompted many expatriates to return.

Real Practices—Case 6	Economic level:	Emerging economy	Business Incubators
US AID Project Fabrykat 2000 in Poland[44]	Organizational level:	Nonprofit	for New Venture Formation
	Technology level:	Medium-tech	

USAID/Poland funded its first technology transfer program from September 1998 to September 2000: Fabrykat 2000. US AID funded the 2-year project to build the Polish manufacturing technology transfer system as a facilitating mechanism to integrate Poland into the EU. The project facilitated the establishment of new Technology Transfer Centers (TTC) in Warsaw and Krakow, trained the Polish TTC management and staff in all aspects of technology transfer operations and program management, provided specialized assistance from US and Polish solution experts to each center's SME clients, while mentoring TTC staff members, and assisted the TTCs in promoting themselves as engines of local and regional economic growth and undertaken activities designed to enhance TTC resources. The program provided technical consulting to 113 SMEs in Poland. It also made available specialized assistance in venture capital, lean and agile manufacturing methodologies, collaboration software and training, technology transfer models, and business planning. The project strengthened the financial, marketing and technical capabilities in four technology transfer centers and also demonstrated the potential of building partnerships and strategic alliances between US firms and Polish enterprises. The experience demonstrated shortened technology transfer cycle and reduced costs through the use of Internet tools.

One of the key lessons of this program is that technology can be both overestimated and underestimated at the same time. There were several cases where the benefits of awareness, availability, and accessibility to the global grid of knowledge experts were apparent, but also non-apparent, elegant, and powerful solutions to challenging technical and business problems were provided quickly via virtual consultation, often, saving travel time and costs. Yet, in some cases, attempting to solve problems only by virtual interaction proved inefficient and ineffective.

Real Practices—Case 7	Economic level:	Emerging economy	Business Incubators
IBI Builds Incubators in the USA for Foreign Firms[45]	Organizational level:	Nonprofit	for New Venture Formation
	Technology level:	High-tech	

[44] US Agency for International Development (USAID) (2002). US AID Mission to Poland: Europe and Eurasia – Manufacturing Technology Transfer Project (Fabrykat 2000). Available: http://www.usaid.gov/pl/fabrykat.htm.

[45] The Information for Development Program (infoDev) (2002). Barbara Harley on the International Business Incubator. *infoDev eXchange* 11, Jan-Mar 2002, 5–8. Available: http://www.infodev.org/exchange/pdf/exch11.pdf.

The International Business Incubator (IBI)—the Business Embassy of Silicon Valley—is a nonprofit business incubator sponsored by a collaboration of business, government and academic organizations. Headquartered in Silicon Valley, CA, it is a technology incubator for international companies; it assists early-stage for-profit companies worldwide and is committed to making its international client businesses a success through growth and strategic partnering. IBI's staff has direct experience with development and implementation of incubator projects, particularly the ones focused on specific technologies and industries or focused on economically disadvantaged populations or responding to the impact of defense downsizing and base closings.

IBI provides the following services:

- Applying the Silicon Valley business model to high-tech startups
- Providing basic incubator services in local clusters, in the USA and internationally
- Providing virtual incubator services to all clients
- Providing specialized advisory services to foreign ventures establishing operations to do business in the USA.
- Providing advisory services to foreign governments to set up incubators of their own, replicating and franchising their winning formula.

In addition to incubator services and training, they also have a Delegation Program, which consists of visits and seminars by consulates, trade missions, US Department of Commerce, academic leaders, and other business incubators from a number of different countries. The media coverage associated with it is a welcome by-product for the startups and the incubator. IBI also provide world-class market research at a much more competitive price. By bridging the information gap, it allows for a substantial reduction in the time-to-market.

Real Practices—Case 8 ZongGuanCun: Virtual Incubators in China[46]	Economic level: Organizational level: Technology level:	Emerging economy Public–private/international Medium-tech	Business Incubators for New Venture Formation

Researchers are advocating government support for a virtual incubator in the Information Technology industry in ZongGuanCun, China. ZongGuanCun is the "Chinese Silicon Valley," located adjacent to Beijing. Nearby are 73 universities and colleges, and a population of over 300,000 students.

Most IT businesses in China are small, due to newness of the technology to China, and predominant platforms are in English. Other challenges the researchers report are global fragmentation of an industry reliant on strategic alliances with outsiders, and a shortage of venture capital in the recently and incompletely liberated

[46] Xu, Qingrui, Caozhi Xu and Jin Chen (2001). A model for virtual incubator. Management school, ZheJiang University, China. In IEEE Sessions – Research Paper Presentations, presented to 2001 IEEE International Engineering Management Conference. Available: http://lallyschool.rpi.edu/ieee/Research%20Paper%20Presentations.htm.

market economy. Only 26 % of Chinese companies have a strategic management plan with an outlook of 5 years or more. In the past, socialist economy planning seldom considered markets. Intellectual Property Rights (IPR) are not enforced or are nonexistent in most areas.

The recommendations advanced by the researchers to the Chinese government include: (1) globalized participation in IT is critical to creating wealth; (2) Government support is needed for alliances with universities, institutes and other companies; (3) the creation and promotion of a venture capital market is urgent; and (4) the creation and enforcement of IPR laws is equally vital.

Their recommendations to Chinese entrepreneurs include: (1) strategic management is the center of enterprise management and risk management in a rapidly changing IT market; (2) human capital and good enterprise culture are critical to support knowledge-based economy; (3) alliances and outsourcing are very important for learning and business development; and (4) the Internet provides a method in IT to build alliances and track market changes unimpeded by geographic barriers.

Real Practices—Case 9 TradenetSL: Virtual Incubator in Sri Lanka[47]	Economic level: Organizational level: Technology level:	Emerging economy Nonprofit High-tech	Business Incubators for New Venture Formation

TradenetSL is the trade information network of Sri Lanka, instituted by the Ministry of Internal and International Commerce and Food in May 1995, to meet the growing information needs of the Sri Lankan business community. The network's primary function is to disseminate trade information to users, both local and abroad. Local users are exporters, business people, governmental policy and decision makers. Foreign users are buyers and investors.

Other objectives of the service include: promotion and popularization of e-commerce in Sri Lanka; facilitating exchange among businesses, consumers, and government; and making electronic communication and Internet affordable to SMEs. Based on the success of TradenetSL, the Export Development Board set up a virtual incubator service called Cyber Trader, which provides a competitive edge to Sri Lankan businesses by linking exporters with buyers overseas, conducting negotiations and executing agreements, accessing legal counsel and management advisory services, arranging travel and meetings, and providing business promotion and information exchange. The next features planned for future transactions are electronic payments and fund transfers.

[47]Gamage, Lalith (1999). E-Commerce in Sri Lanka. In *Electronic Commerce and Developing Countries,* presented to UNDP, UNCTAD, IICD, and World Bank/infoDev, 10–17 October 1999, Geneva. Available: http://www.undp.org/info21/telecom99/Booklet.pdf.

Real Practices—Case 10	Economic level:	Developed country	Business
Microsoft Incubator for Video Game Development[48]	Organizational level:	For-profit	Incubators for New Venture Formation
	Technology level:	Medium-tech	

The Xbox Incubator Program is part of Microsoft's commitment to support the video game development community, in alignment with strategy to enlarge its presence in the video game market. This unprecedented program is available to game developers who want to commit resources to developing an Xbox game for licensed use on Microsoft's proprietary game console.

Participants must use an official Xbox Development Kit (XDK) before securing relationships with major publishers. Microsoft provides independent game developers access to XDKs and technical support. Only games created with the XDK and distributed by licensed publishers will be available as commercial products.

Real Practices—Case 11	Economic level:	Developed country	Business Incubators for New Venture Formation
MedMined, Inc.: Award-Winning Incubator Client Firm in Alabama[49]	Organizational level:	For-profit	
	Technology level:	High-tech	

MedMined, Inc. is the winner of the 2002 Outstanding Incubator Client in Technology Start-up Award, sponsored by the National Business Incubator Association (NBIA). MedMined is a client of the Office for the Advancement of Developing Industries (OADI) Technology Center, at the University of Alabama at Birmingham.

The company developed customized and proprietary data-mining technology to track patterns of hospital-acquired infections and to identify when infections become drug resistant. The founder formed MedMined in January 2000, leveraging research he had performed as a graduate student 12 years prior. The company moved operations into its incubator office in April, 3 months later. Within a year, the company began offering services commercially, and received $2 million in venture capital funding.

Locating in the incubator provided resources to focus better on this startup's business—providing contacts in the hospital industry and opportunities to present to venture capitalists. First year revenues were $5,000. 2001 revenues increased to $135,000. 2002 revenues estimated at over $500,000. MedMined was also named among the top five healthcare startups by Fortune Small Business Magazine in January 2003.[50]

[48]Microsoft PressPass (2000). Microsoft Embraces the Worldwide Independent Video Game Developer Community Company Announces Xbox Independent Developer Program And Xbox Incubator Program. Available: http://www.microsoft.com/presspass/press/2000/Nov00/XPKPR.asp.

[49]National Business Incubation Association (NBIA) (2003). 2002 Outstanding Incubator Client Award Winners - Outstanding Incubator Client: MedMined Inc. Available: http://www.nbia.org/awards_showcase/2002/2002_client.php.

[50]Fortune Small Business (2003). Big Ideas 2003: 14 Hot Startups – MedMined, Keeping hospital infections at bay. Available: http://www.fortune.com/fortune/smallbusiness/articles/0,15114,417664-4,00.html.

Real Practices—Case 12	Economic level:	Developed country	Business
FAME Renaissance: Technology Incubator for Impoverished Communities in Los Angeles[51]	Organizational level:	Nonprofit	Incubators for New Venture Formation
	Technology level:	Low-tech	

FAME Renaissance is a nonprofit economic development initiative of The First African Methodist Episcopal (FAME) Church, located in Los Angeles. Established as an affiliate of the First AME Church in 1992, FAME Renaissance operates several major social and business development programs designed to create wealth in impoverished communities within Los Angeles County. The primary mission of FAME Renaissance is to create jobs and business opportunities by forming public and private partnerships.

FAME's organizers have found that companies are leveraging opportunities in technology—Internet, satellite, sophisticated multimedia software—to reshape the business environment, to create wealth and jobs across the nation, to expand into new markets, to increase business productivity, and to grow customer satisfaction. The FAME Renaissance Business Incubator targets emerging growth firms in multimedia and subsidiary sectors, to support entertainment technology commerce in South Central Los Angeles.

The incubator program tracks the progress of participants from entry through graduation. Prospective entrepreneurs and business owners receive a thorough analysis of their business plan and entrepreneurial skills to determine at which level they enter the program. Working with experienced advisors, one for each major business area—marketing, sales, technology, finance/accounting, and legal—entrepreneurs set milestones for their companies growth. Frequent periodic reviews are designed to guide young companies through the first critical stages of business growth by developing a customized 3-year business growth strategy for each Incubator client. The strategy includes business growth targets designed to help clients reach or exceed $1,000,000 in annual revenues and create up to 12 jobs. Graduation policy requires that clients achieve these targets and complete the program within 3 years.

Incubator resources include access to internal and external investment funds and other capital, a fully equipped computer and Internet lab, a business library and information center, and flexible participation options that include occupancy (tenant) and non-occupancy (affiliate) options. A key part of the program is a focus on personal development of the entrepreneurs, who are initially selected in part by their willingness to engage in FAME social contract. The incubator has created a supportive and nurturing environment for entrepreneurs to learn from one another, the FAME Renaissance team, and from corporate leaders. Client companies are clustered in similar fields to collaborate on such things as contract and funding opportunities, business partnerships and equipment purchases. The incubator conducts training seminars every month, matching entrepreneurs with established leaders in their respective fields to mentor and teach them.

[51]FAME Renaissance Center (2001). An Introduction to FAME Renaissance. Available: http://www.famerenaissance.org/about.htm.

Real Practices—Case 13	Economic level:	Developed country	Business Incubators
National Business Incubation Association (NBIA)[52]	Organizational level:	Non-profit	for New Venture Formation
	Technology level:	High-tech	

The National Business Incubation Association (NBIA) is the World's leading organization for advancing business incubation and entrepreneurship. This not-for-profit professional association is composed primarily of incubator developers and managers, technology commercialization specialists, educators and business assistance professionals. NBIA assists early-stage companies worldwide, providing training and information on incubator management and development. The association also conducts research, compiles statistics and produces publications on approaches to developing and managing effective programs. Administrators track relevant legislative initiatives and maintain a speakers' bureau and referral service. NBIA creates partnerships with leading private-sector and public-sector entities to further the interests of the industry and its members

Objectives of the NBIA include: providing information, research and networking resources to help members develop and manage successful business incubation programs; monitoring and disseminating information about industry developments, trends and best practices; informing and educating leaders, potential supporters and stakeholders of the significant benefits of business incubation; building public awareness of business incubation as a valuable business development tool; expanding capacity to create valuable resources for members through partnerships; engaging and representing all segments of the business incubation industry; and creating value for members.

Throughout the year, NBIA engages in many activities to support members' professional development. These include: organizing conferences and specialized trainings; producing publications that provide hands-on approaches to business incubation; conducting research and compiling statistics on the incubation industry; supporting an annual awards program that recognizes outstanding member incubators, clients, and graduates; sponsoring forums to enhance members' networking and information-sharing opportunities; and coordinating an international consulting service to contribute to sound incubation program development and management worldwide.

Real Practices—Case 14	Economic level:	Developed country	Business Incubators
TEDCO: Business Incubators for Technology Transfer in Maryland[53]	Organizational level:	Public–private	for New Venture Formation
	Technology level:	High-tech	

The Maryland Technology Development Corporation (TEDCO) is a business incubator and cluster network to facilitate the creation of businesses and foster their growth through the development and transfer of technology. The Corporation was created by the State legislature in 1998, as a "body politic and corporate, … constituted as a public instrumentality of the State." Governed by a 15-member Board,

[52]NBIA, op. cit.

[53]Maryland Technology Development Corporation (TEDCO) (2002). Maryland's Business Incubators: Angels and Eggs. Available: http://www.marylandtedco.org/programs/incubator/AngelsEggs.pdf.

appointed by the Governor with advice and consent of the Senate, the Board is comprised of leaders in the State's technology community and contains representatives from these sectors: private, university, nonprofit, and public.

TEDCO's vision is to make the State of Maryland internationally recognized as one of the premier twenty-first-century locations for technology and technology-based economic development. To respond to the needs of the R&D community, TEDCO establishes and manages programs that fill gaps in the innovation process—focusing on those critical areas where the organization can add unique value—operating in partnership with other organizations through a flexible, technically oriented professional staff.

TEDCO program goals include: enhancement of the transfer of technology from universities and federal laboratories to the private sector to foster the growth of innovative companies, in critical or high growth sectors; extending the benefits of technology to all communities, companies and citizens in the State; and increasing the State's visibility as a premier location for technology-based economic development. To achieve this, the Corporation leverages resources with private sector firms, with government agencies at the federal, state and local levels, and with various foundations. These entities work in partnership to plan, develop and deliver an integrated set of technology programs and professional information on technology policy to public/private decision makers.

TEDCO really has attained prominence as a prolific energizer of technology licensing and commercialization. Within 3 years of inception, businesses graduating from the incubator program generated nearly $500 million in gross state product and close to $100 million in taxes, while creating thousands of technology-sector jobs. Figure 2.15 shows the top five highest priorities for incubator companies are Internet access, linkages to investors and lenders, access to experienced individuals for the formation of management advisory boards, and planning and securing facilities.

Real Practices—Case 15	Economic level:	Developed country	Business Incubators
Arno Valley Technology Clusters in Italy[54]	Organizational level:	Public–private/ international	for New Venture Formation
	Technology level:	High-tech	

Arno Valley, Italy is host to a cluster of SMEs, primarily producers of ICTs. The technology cluster is localized along the Arno River in the metropolitan areas of Firenze-Prato, Pisa, Livorno, Arezzo, and Siena. This cluster has been studied to ascertain the characteristics of high-technology new ventures and the common factors that the entrepreneurs of such ventures would advocate to elevate the opportunity for success.

For businesses participating in this local cluster, entrepreneurial capacities are defined in an extremely specific and idiosyncratic way. Creation of new companies positively depends on the capacities that the territorial systems have developed to function, based on incubators of knowledge necessary to forge and prepare the potential base of new entrepreneurs. Companies operating in knowledge-intensive

[54]Boscherini, Fabio (2003). Study of the Creation of New Enterprises in Italy.

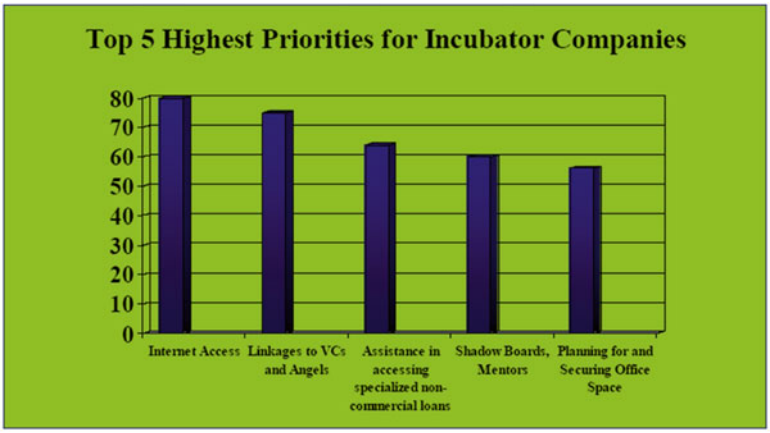

Fig. 2.15 Top five highest priorities for incubators companies

sectors are localized in the principal metropolitan areas of the region. In the knowledge-intensive sector, the entrepreneurial processes led to the creation of new companies that are not tied to the continuity of former companies—that is, the entrepreneurial project leading to the creation of a new company is original. In the knowledge-intensive sector, the creation process takes an individual and introverted path. Businesses take advantage of opportunities perceived in new markets and externalities of the large-scale innovation system (universities, public research centers, and large high-tech companies).

In the entrepreneurial process, in addition to the environment the relevance of the innovation system stands out. The differences observed in the entrepreneurial processes that have been studied in Arno Valley depend as well on the presence of two distinct innovation systems existing in Italy: the SME circuit, and the circuit of large-scale research. Among the critical success factors promulgated are: foster actions oriented towards the production of academic spin-offs and entrepreneurial spin-offs, strengthen the education system; define programs for assistance and training in entrepreneurial functions; and promote venture-capital actions.

2.3.12 Real Practices Case Studies in the Use of ICT to Support and Promote SMEs

Real Practices—Case 16	Economic level:	Developing country	ICT to Support
Phone and Fax for Village Sunglasses Maker[55]	Organizational level:	For-profit	and Promote
	Technology level:	Low-tech	SMEs

[55]Duncombe, Richard and Richard Heeks (2001). Case Study 1: How telephone/fax can support a micro-enterprise. *Information and Communication Technology: A Handbook for Entrepreneurs in Developing Countries,* p. 5. Available: http://idpm.man.ac.uk/rsc/is/ictsme/entrephbk/.

Among its many functions, the UK Institute for Development Policy Management (IDPM) supports entrepreneurial enterprise through ICT in developing countries. The Institute recently reported this case example involving a village micro-enterprise.

An entrepreneur and two part-time market sellers make and sell sunglasses. Nearly half of their customers come from the local community, and customers from outside usually come on weekends. The entrepreneur has advertised the business in his village, and has a sign outside. He depends on the market sellers to reach customers outside the village. He would like to go out and do more selling, as his market sellers really do not know the technical side, but he cannot leave his business premises easily, due to fear of losing customers because he is the only one who can make the sunglasses, and he is partly disabled following polio.

Personal contact with individual customers is essential but the entrepreneur uses a local community phone/fax facility to keep in touch with his suppliers; the lenses for the glasses come from a neighboring country. From this shared link he not only controls supplies—and is able to restock quickly—but he also receives good information that he can use to increase sales, such as catalogues and information on new styles of frames that he can share with customers. Without access to phone and fax, he would face high supply costs and long absences from his work.

He would benefit even more from a phone/fax in his own premises. He could avoid leaving his premises—an inconvenience given his disability. There is also the danger of losing sales while he is away using the community facility. It would also mean more satisfied clients—for customers traveling from outside the village, initial contact could be made by telephone to check if the trip was worthwhile.

Real Practices—Case 17	Economic level:	Developing country	ICT to Support
Ecosandals.com: The Internet Brings Global Market to Sandal Makers in Kenya[56]	Organizational level:	For-profit	and Promote SMEs
	Technology level:	Medium-tech	

A micro-enterprise in Korogocho, Kenya manufactures high-quality rubber sandals by recycling tires, which they sold locally in this impoverished city of 400,000 from the period 1995–2000, employing four workers.

In 2001, the project went online. Within a month, orders were coming in from around the World, and within a year, the demand had increased sixfold. As of mid-2002, the production team in Korogocho had expanded to 27: 9 young mothers and 18 young men. These young adults had all dropped out of school for lack of fees, and without this employment might otherwise be scavenging for less than a dollar a day—a typical economic condition in this distressed area of Kenya, one of the World's poorest.

[56]The Information for Development Program (infoDev) (2002). Learning Lessons from ICT Stories: Ecosandals.com. *infoDev eXchange* 12, Apr-Jun 2002, p. 8. Available: http://www.infodev.org/exchange/pdf/exch12.pdf.

Sandal makers earn a minimum of 30 % of profit on each sale, which can be as much as 480 shillings ($6), having a substantial impact on the producers' lives and livelihoods. All sandal-makers have access to the Internet, and in addition to their productive, gainful employment, all are learning basic computer, math, and language skills, as well as online marketing. The project continues to grow and provide resident participants with steady income, training, computer literacy, and a reliable working environment. They now produce a bi-monthly newsletter, distributed to 55 countries.

This village micro-enterprise has "gone global." ICT turns the formula of development upside down. Korogocho residents operate in an online world where they produce and sell quality footwear, author a newsletter that is sent across the world, and correspond with and educate customers sitting in more developed nations. The sandal-makers are "the helpers" and their customers abroad are "the helped." Globalization need not be just about the big multi-national corporation that dominates, educates and dictates to the little developing country. It also can be about the little multi-national corporation dictating terms of sale to customers in far more developed settings.

Real Practices—Case 18	Economic level:	Developing country	ICT to Support and
Radio Sagarmatha: A Radio	Organizational level:	Nonprofit	Promote SMEs
Station Broadcasts the Internet in Nepal[57]	Technology level:	Low-tech	

Radio Sagarmatha was the first community FM radio in South Asia, broadcasting in the Kathmandu valley. In Nepal, radio is the ubiquitous medium—low cost, and literacy is not a barrier. Nepal was connected to the Internet in 1995, but a majority of the population cannot benefit due to higher cost, low availability, lack of exposure, and a minimum working knowledge of English.

In early 2000, the station devised an IT-related program with the radio show to act as an interface between the users and the Internet. More than 100 episodes have been broadcast, in an evolving format that has included: describing Web sites while browsing the Internet, explaining technical jargon, talking with experienced users to learn ways to get information from the Internet and ways to get practical benefits from that information, live open-format request lines, and most recently, a radio quiz.

The Computer Association provided a grant to increase the airtime, and most efforts have been voluntary, for the larger public good. Support has been notable. At least one listener wrote, "If it is financial problems, we can form a listeners' club to sustain the program." The latest addition to the program, the radio quiz, generated increased interest and garnered promotional gifts from the IT industry, including free training for winners, which in turn catalyzed user interest.

[57]The Information for Development Program (infoDev) (2002). Learning Lessons from ICT Stories: Marrying Radio with Internet in Nepal. *infoDev eXchange* 12, Apr-Jun 2002, p. 9. Available: http://www.infodev.org/exchange/pdf/exch12.pdf.

The definite result has been the proof of concept. Taking ICT to people does not necessarily mean putting a computer into every village. What is first needed is to take the information that can make a difference. ICT is not an end in itself, rather, it is a tool that needs to be adapted for local use.

Real Practices—Case 19	Economic level:	Developing country	ICT to Support
Kabissa.org: Web Mail Services are Delivered Throughout Africa[58]	Organizational level:	Nonprofit	and Promote SMEs
	Technology level:	Medium-tech	

Kabissa.org delivers Web mail services throughout Africa. The concept originated in Nigeria in 1998, to provide human rights groups with access to e-mail, for improved reporting of human rights abuses. Organizations were desperate for capacity building, training, and access to the net. Kabissa was set up on a nonprofit basis, headquartered outside of Africa, to ensure that nonprofit organizations throughout Africa working in improving the lives of people in Africa may have a presence on the Internet.

Without advertising and other hidden costs, organizations are able to access space on the Kabissa server, with costs recovered through donations and provision of additional features such as domain hosting, mailing lists, and online databases. African organizations have serious difficulty accessing the Internet reliably; many do not have access to computers, and they often have no telephone service or power. Kabissa began offering access to net resources via e-mail: users can send the Internet address of an online resource to an e-mail box, and get a copy of the resource returned to them via e-mail, so they can plan their Internet research and spend less time online.

Kabissa joined forces with other NGOs to publish a social justice newsletter delivered weekly via e-mail. Development professionals in very remote areas get information and answers to their questions on a timely basis via a range of topical e-mail newsletters and a mail server. From remote villages with no phone lines, users can travel to collect their e-mail on diskette to take with them, and likewise send e-mail messages from diskette they have brought from the village. As of mid-2002, Kabissa serves over 300 member organizations in 32 African countries.

Real Practices—Case 20	Economic level:	Developing country	ICT to Support
Quipunet: Web Service Connects Peruvians Around the World[59]	Organizational level:	Nonprofit	and Promote SMEs
	Technology level:	High-tech	

[58]The Information for Development Program (infoDev) (2002). Learning Lessons from ICT Stories: Kabissa – Space for Change in Africa. *infoDev eXchange* 12, Apr-Jun 2002, p. 10. Available: http://www.infodev.org/exchange/pdf/exch12.pdf.

[59]Davies, Martha (1999). Amidst the riches available – we are still very poor. In *Electronic Commerce and Developing Countries,* presented to UNDP, UNCTAD, IICD, and World Bank/ infoDev, 15–16 October 1999, Geneva. Available: http://www.undp.org/info21/telecom99/Booklet.pdf.

Quipunet is a virtual organization for global Peruvians—a forum designed to connect citizens abroad to home, and bring information access to rural Peru. The service was inspired by spiraling growth of the Internet. Founders thought they could just connect and send information galore, but they have been daunted by challenges. Despite the lack of reliable infrastructure, and unanticipated learning curve, through sheer perseverance and determination Quipunet's members have achieved a great deal of progress. They have learned to host virtual seminars and to work with virtual, global teams. They have trained users in Internet tools. They have creatively incorporated alternative methods of communication to encompass people without direct online access.

Of the many obstacles encountered, language barrier was among the highest, as this impacted even those who served as pivotal nodes. "Countries that do not know English is like entering a candy store with your hands tied behind your back, being able to see, and not touch, tantalized by all the information available," said one founder. Content would need to be sent out for sector specific translation, as the vocabulary of particular sources would contain so many unfamiliar technical terms. The infrastructure of the rural places was poor, or in most cases nonexistent, and connectivity, where available, was very expensive.

Real Practices—Case 21	Economic level:	Developing countries and emerging economies	ICT to Support and Promote SMEs
Development Gateway Foundation Delivers Knowledge[60]	Organizational level:	Public–private/international	
	Technology level:	Low-tech	

The Development Gateway Foundation is a not-for-profit organization operating internationally to reduce poverty and to support sustainable development through the use of ICT. The Foundation administers four programs. (1) The Development Gateway Portal is an interactive portal for knowledge sharing on sustainable development and poverty reduction. (2) Network Research and Training centers can be located, including networking hubs in the developing world, which serve for the exchange of ideas and testing ICT applications to benefit the poor. (3) The Grants and Investments program supporting ICT for development projects and programs at the local, national, regional, and global level. (4) The ICT Development Forum is for discussion of ICT for development issues, and the promotion of partnerships and synergies between public sector, private sector, and civil society.

The Development Gateway Portal provides a platform for information and knowledge exchange for the global community of development practitioners in four broad areas: Development topics; AiDA (Access information on Development Activities); dgMarket (for government procurements); and Country Gateways (national initiatives on local development). The aggregate benefits of these programs include shared information, communities of practice, partnerships, better coordination, and standards for information sharing.

[60]Development Gateway Foundation (2003). Available: http://www.dgfoundation.org.

Real Practices—Case 22 **UK Institute for Development Policy Management (IDPM) Supports ICT in SED in Developing Countries**[61]	Economic level: Organizational level: Technology level:	Developing countries Public–private/international Medium-tech	ICT to Support and Promote SMEs

Among numerous functions The UK Institute for Development Policy Management (IDPM) supports ICT within small enterprise development (SED) to further international development targets. The Institute advocates four functional "Action Areas" for ICT and SME development: (1) ICT as an enterprise output—SMEs producing hardware, software, and telecommunications products; (2) ICT as a primary, processing technology—SMEs providing data entry services, ICT-based business services, software customization distance learning, etc.; (3) ICT-related support activities—computer training, consultancy, content provision, and other services; and (4) ICT as a secondary processing technology—covering communication (e-mail/Internet/mobile), data processing (small business information systems), and ICT-based manufacturing systems.

The first three of these categories encompass the ICT sector and are primarily concerned with the production of ICT goods and services. The fourth category includes all other SME sectors that are ICT consumers. ICT provides the most direct benefit (employment, growth and local capacity) within the ICT sector itself (Action Areas 1–3). Action to support the local ICT sector should, therefore, be a priority to government, private enterprise and NGOs—particularly those concerned with implementing ICT within wider poverty alleviation programs, specifically in health, education, environment, and governance. In most low-income developing countries, ICT-sector support should focus on Action Area 2 and 3—primarily digital products, software customization, ICT-based services, training and consultancy, and other ICT-based business services. In large and/or industrializing developing countries, there will be more scope to focus on Action Area 1—manufacturing computer hardware, telecom products and computer software. ICT also provides considerable indirect benefit to other sectors (Action Area 4) by improving the efficiency of business processes and through enabling SMEs to develop new products and services

Mechanisms for support will be country specific. There is little experience amongst donors in project support, either in the ICT-sector itself or amongst secondary users, but general requirements for policy/project support apply. The mission success formula demands support at all levels.

For enterprise-level support, enterprises may have little need for direct business assistance, but can benefit through policy measures that facilitate access to finance, reduce the cost of access to infrastructure, support skills and technology, and create

[61] Duncombe, Richard and Richard Heeks (2001). Enterprise Development and Information and Communication Technologies in Developing Countries: Supporting "ICT-Flyers" – Executive Summary 2001. Available: http://idpm.man.ac.uk/ictflyer.html.

market access (through linkages and vendor development programs). For intermediary level support, commercially based organizations will be the most effective intermediaries, specifically sector-based trade associations and chambers of commerce at the local level, and umbrella and employers associations at the national level. In the ICT-sector it is important that intermediaries are supported that represent the local industry, and not other academic or governmental/NGO interests. Other critical intermediaries will offer technical support—such as suppliers and other institutions facilitating technology and management development. For policy level support, most low-income developing countries have no strategic ICT policy. There needs to be support for strategic policy development that includes the ICT sector and secondary users. Overall, national policy should be directed at improving technical and data infrastructure, facilitating access to technology and networks and the enhancement of ICT skills.

The IDPM reports a particular caution pertaining to "digital-divide" issues. Digital divide is the term given to the dichotomy of technological access: those who have access have access to much, and those whose access is limited have very little at all. To ameliorate this divide, policy must also address ownership and transfer of knowledge and know-how. ICT is a technology-based means of transmitting information, enhancing knowledge, increasing productivity, or creating new products and services. The success of ICT in developing countries will be critically dependent on know-how and skills capacity—technical, managerial, and developmental—both within the local ICT sector and among secondary ICT-users.

Real Practices—Case 23 ISP Competition in Romania[62]	Economic level: Organizational level: Technology level:	Developing country Public–private/international High-tech	ICT to Support and Promote SMEs

The Romanian National Agency for Communications and Informatics (NACI) set a deadline prior to 2002 for liberalization of the public telecommunication network by 2003. Anticipating the entry of competition for the first time in its history, The RomTelecom operator, fully privatized but in a monopolist position, increased tariffs in 2001 by almost 8 %.

As a result of widespread criticism in media, the Romanian Senate established a commission to investigate the privatization of RomTelecom and the consequences for the economy and national security. The World Bank was in the preliminary stages of examining the potential in the developing communications market in Romania. It was intended that this would lead to further development of Internet connections, which were discouraged at the time by the telecom network, by both quality and price. Estimates showed that for every dollar paid to the Internet service provider, RomTelecom received three dollars!

[62]European Survey of Information Society Projects and Actions (ESIS) (2001). Regulatory Developments: Romania Update memo – January 2000. Available: http://www.eu-esis.org/esis2reg/ROreg3.htm.

As a result of investigations, the incumbent RomTelecom was prevented from participating in the ISP market. This made the data/Internet market open for competition and permitted means of alternative connectivity, such as cable, VSATs, private networks, leased lines, etc. Strong demand from the public (mainly in the age group of 15–35 years) caused increased competition on the ISP market. Competitive forces caused the cost of an hour on the Internet to drop by half from 2001 to 2002. The same competition between ISPs led to the declaration of increased numbers of users, just to gain the confidence of the public. The free-market condition continues to improve.

Real Practices—Case 24	Economic level:	Emerging economy	ICT to Support
Jhai Foundation: Peddle-Powered Internet in Laos[63]	Organizational level:	Nonprofit	and Promote
	Technology level:	Low-tech	SMEs

Lacking phone lines and electricity, some Laotian farmers conceived a means for Internet access while talking with development workers from the Jhai Foundation, a San Francisco nonprofit group. The prototype is a computer (the only one in the village, bolted to the floor of a public building, to prevent theft), hooked to a bicycle-powered generator and a set of wireless antennae, all fabricated from spare parts.

Laos is a brutal place to farm, littered with Vietnam-era unexploded ordnance and racked by a dusty dry season. The farmers wanted Internet access to track weather movements and price swings in rice, allowing them to optimize the scanty profits from their crops. They also want to keep in touch with their families, who may have left the bombed villages, and have not had contact for 25 years.

The group is cobbling together five inexpensive computers with out-of-date microchips. The computers are linking to the Internet via wireless broadcasting stations costing only a few hundred dollars. A tower located in a Laotian city will tap into the Net and the local phone system, then repeat the signal toward villages equipped with similar wireless repeater towers, without expensive satellites or copper-wire phone lines.

Development groups are watching the project closely. The farmers are effectively bicycling from the nineteenth century to the twenty-first.

Real Practices—Case 25	Economic level:	Emerging economy	ICT to Support
Inter-American Development Bank (IADB) Promotes Development in Latin America[64]	Organizational level:	Public–private/international	and Promote
	Technology level:	Medium-tech	SMEs

[63]Thompson, Clive (2002). The Pedal-Powered Internet. *The New York Times Magazine,* December 15, 2002. Available: http://www.nytimes.com/2002/12/15/magazine/15PEDA.html?ex=1056945600&en=90b822dfae35d010&ei=5070.

[64]Garrett, Andrés (2003). ICT for Development in the Latin American and Caribbean Region: An Integrated Process of Stakeholder Participation. In *Enterprise Latin America ICT in Latin America: Business Partnerships in Development Conference,* presented Sao Paulo, Brazil, February 25, 2003.

At the beginning of 2003, the Inter-American Development Bank (IADB) set forth its latest policy position in the use of ICT for development in the Latin America and Caribbean Region. The Bank proposes to facilitate access for IADB borrowing member countries to state-of-the-art ICT and expertise, intending to enhance local and regional development programs and achieve a greater efficiency, reach and impact of such efforts. They project that freer access will increase competitiveness, promote an efficient, equitable, and sustainable development, contribute to social equality, and reduce vulnerability to economic crises.

There are three specific IADB strategic "Action Areas" regarding ICT: (1) ICT in sustainable economic growth; (2) ICT in promoting equity and poverty reduction; and (3) ICT in governance. The best practices envisioned by IADB are as follows.

Action Area 1—To foster sustainable economic growth: Enhance capacity of borrowing member countries to deploy ICT to accelerate the process of economic growth and wealth creation; contribute to the promotion and development of electronic business and electronic commerce to enhance competitiveness in the new knowledge economy; contribute to the incubation of new technology-based enterprises; and facilitate the access to emerging technologies by SMEs.

Action Area 2—To promote equity and poverty reduction: Promote human capital formation and social development through the deployment of ICT in lifelong learning in the knowledge economy; implement connectivity and community outreach programs, including telecenters; and implement ICT for human enhancement programs, addressing gender issues in knowledge economy, integrating marginal and geographically distant populations.

Action Area 3—To introduce and champion e-governance: Deploy ICT in support of new patterns of cooperation among public, private, and civil society sectors as means to consolidate the democratic process in the Region; facilitate the design, implementation and deployment of electronic government solutions as integral part of an effective modernization of the state process; and enhance the efficiency and accountability of the public administration through ICT

Real Practices—Case 26 Technical Cooperation Activities in Korea[65]	Economic level: Organizational level: Technology level:	Developed country Public–private Medium-tech	ICT to Support and Promote SMEs

Korean researchers conducted a statistical analysis in 2001 to examine changing patterns of technological cooperation activities in the Korean telecommunications sector. The study reports that patterns of technological cooperation activities differ in terms of motivation, the extent and diversity of use, and partners, along technological development stages. Moreover, the impact of each technological cooperation activity on the firm's technological performance varies also along development stages. A technological cooperation activity in this context represents a collaborated

[65]Chung, Jin-Woo, Zong-Tae Bae, and Ji Soo Kim (2003). Changing patterns of technological cooperation activities of innovative small firms along technological development stages in the Korean telecommunications sector. *Technovation*, 23 (2003) 163–173. Elsevier Science Ltd.

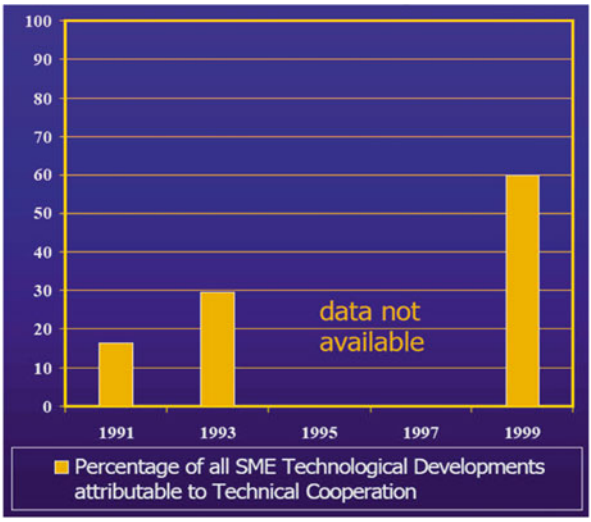

Fig. 2.16 Percentage of all SME technological developments attributable to technical cooperation

project involving SMEs in partnership with other firms, universities, or research institutes, and includes SME firms from both developed countries and developing countries in transnational collaboration with entities from developed countries.

The reported statistics substantiated the following salient conclusions: SMEs generally lack financial, technical, and managerial resources compared with larger firms; SMEs need to acquire technological knowledge from outside sources to supplement their narrow base; and technological cooperation with other firms, universities, and research institutes increased for the Korean ICT sector over the preceding decade. The increasing trend of the percentage of all SME technological developments attributable to technological cooperation activities is shown in Fig. 2.16.

Real Practices—Case 27	Economic level:	Developed country	ICT to Support
PRSource.com: Online Public	Organizational level:	For-profit	and Promote
Relations Service Company[66]	Technology level:	Low-tech	SMEs

PRSource.com is designed to operate as a full-service, virtual public relations firm, offering a complete package of public relations services while assisting clients in communicating their messages to target audiences. This virtual PR firm boasts that it will afford self-directed public relations campaigns at a fraction of the traditional cost. Promoters suggest that traditional PR is about personal relationships and handshakes, while online PR is a tool that allows an individual or company to get their message out to large or small audiences very economically.

[66]ibiz Interviews (2003). Traditional PR vs. online PR. Available: http://www.ibizinterviews.com/silasd1.htm.

With PRSource.com, the client selects and pays for only the PR needs that make the most sense for an individual PR campaign. For its "re-launch" promotion, PRSource has garnered US $1.2 million in cash and business service commitments from e-Conception, a Tennessee technology incubator.

Real Practices—Case 28	Economic level:	Developed country	ICT to Support
NTT DoCoMo, Inc. Venture Transforms Multimedia Market in Japan[67]	Organizational level:	For-profit	and Promote
	Technology level:	High-tech	SMEs

NTT DoCoMo, Inc. is the largest mobile communication carrier in Japan, and has engineered some eminent economic transformations in that country's mobile multimedia business. The company's "i-mode" innovation evolves wireless portable phones into wireless portable information terminals. The Japanese are about 2–3 years ahead of the USA and EU in the use of this technology.

DoCoMo's company leadership saw astounding growth in the mobile phone market and predicted rapid saturation of voice-only devices and services. They made strategic plans to shift market emphasis from volume to value, representing a foray into market "white space," where, at the time, neither supply nor demand were more than hopeful assumptions. To parlay their vision, DoCoMo created a paradoxical organization structure to advance and control the creative destruction of market infrastructure from multiple vantage points. This new venture, the Gateway Business Department (GBD) was a 70-person venture appointed in 1997 with the mission to birth the new market through a process termed Strategic Community Creation.

Simply stated, the company launched a separate enterprise to directly compete with DoCoMo's existing technology platform, with the strategic intention of rendering the present market obsolete. The objective was to move DoCoMo out of a field of many contenders and into the forefront as the parent of the first-to-market leader as the white space is filled in.

There were many challenging dimensions to this willful upheaval of infrastructure. Handsets and transmission hardware needed enhancement. Software needed to be developed for operating units, network and system components. Content attractive enough to stimulate demand had to be constructed and delivered. The significance of Strategic Community Creation is that all of these integral contributions come from other firms that are themselves linked to the present market, and to peripheral markets, all of which stood to gain or lose from the GBD i-mode venture. Success was secured by alliance and positive interplay, in which the majority of actors elected to move together, to share constructively in a larger market. Figure 2.17 depicts the structure of the GBD and its strategic community interrelationships.

[67] Kodama, Mitsuru (2003). Transforming an old-economy company into a new economy——the case study of a mobile multimedia business in Japan. *Technovation*, 23 (2003) 239–250. Elsevier Science Ltd.

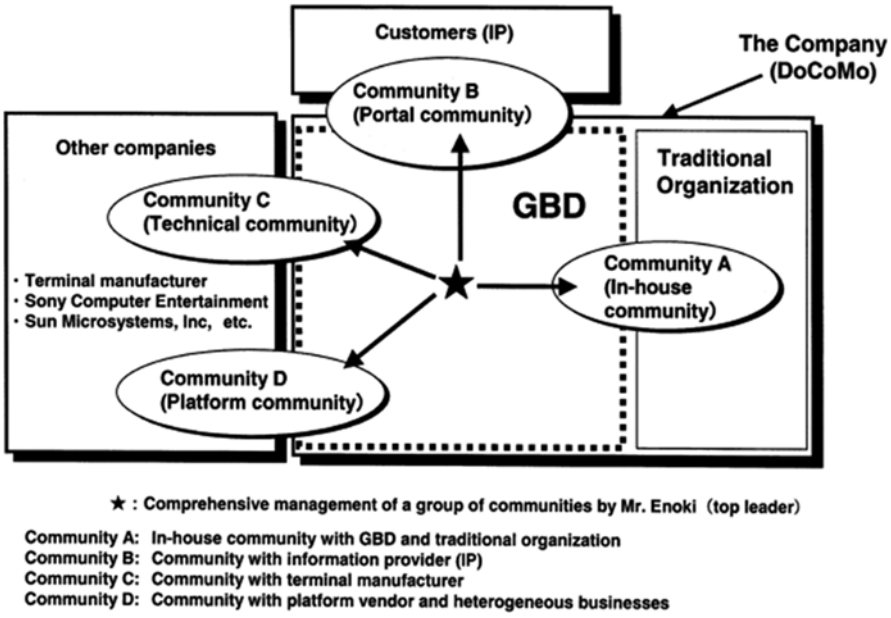

Fig. 2.17 Strategic community creation at GBD

Real Practices—Case 29	Economic level:	Developed country	ICT to Support
End Time Harvest Ministries (ETHM): Enterprise Training for Urban Revitalization in Maryland[68]	Organizational level: Technology level:	Nonprofit Medium-tech	and Promote SMEs

End Time Harvest Ministries (ETHM) is a non-denominational faith-based organization that serves the Port Towns district of Prince George's County, MD and adjacent neighborhoods. Bordering Washington DC, these communities have been marked as economically distressed zones in need of redevelopment assistance by local and state authorities, and by the US Census Bureau. ETHM establishes and administers local programs to assist the needy: homeless and indigent families, at-risk youth, and elderly shut-ins. The Ministry works in alliance with neighborhood businesses, churches, schools, and town councils to deliver its voluntary public services. As a nonprofit organization, ETHM receives funding in the form of grants from government sources and charitable donations from commercial contributors and other NGOs.

[68]Personal communication, Rev. Gail Addison, Executive Director, End Time Harvest Ministries, Inc.

Building on their success in youth intervention and employment campaigns, ETHM has undertaken a new initiative: an entrepreneurial training center to help revitalize the neighborhood and to enlarge and enrich ETHM's successful Jobs-for-Youth Program. To construct this Community Entrepreneur Institute, a vacant warehouse is to be renovated for classrooms, ICT labs, and supporting service offices. Volunteers and professional educators will provide training to youth and unemployed residents in life skills, business competencies, and management principles, with an eye for grooming local talent to start businesses of their own, also preferably within the nearby community. The Ministry's vision is for positive intervention and development, starting at the earliest age and as close to home as possible.

In support, Hewlett-Packard/Compaq has donated PCs and peripherals to equip the ultramodern training labs, and the County Executive's office is championing the venture as a model for economic healing. Coalitions of residents, business owners, elected officials, school administrators, and parents are working to obtain State support and funding to make the Community Entrepreneur Institute a national showcase.

Real Practices—Case 30 Telecottage: Telecenter for e-Development in Rural Australia[69]	Economic level: Organizational level: Technology level:	Developed country Public-private/international Low-tech	ICT to Support and Promote SMEs

Australia's rural sector is experiencing a great crisis both economically and socially due to the prolonged drought and low commodity prices. Australian Government has been implementing various types of programs to adjust and revitalize the rural industries and communities. Recent developments in ICT offer a great opportunity to facilitate the rural adjustment and development process in Australia. Obtaining access to new technology is often difficult for people in rural communities because they have much less opportunities to access to it compared with their urban counterparts.

Australia has been experimenting with several programs to enhance ICT in rural areas. Among other things, the telecottage concept has been focused on by government and communities. Telecottage (telecenter) is a new approach to rural development using ICT. The world first telecottage was set up in a small village in rural Sweden in 1985, and the idea has been adopted by a number of countries around the world. In 1992, the Australian Federal Government commenced the Telecentres Program, which aimed to assist rural and remote communities to establish and operate community facilities where all people could gain easy public access to computers and information technology for education, training, and enterprise purposes.

There are currently about 120 telecenters in rural Australia, with funding from a range of Federal, State, local government and community sources. The Australian Rural Telecentres Association has been formed at the national level to promote networking of these facilities.

[69] Suzuki, Atsushi and Shankariah Chamala (1998). Role of Telecentres in Rural Development in Australia. Available: http://www.jsai.or.jp/afita/afita-conf/1998/P08.pdf.

Real Practices—Case 31	Economic level:	Developed country	ICT to Support
Welsh Development Agency (WDA) Promotes ICT for SMEs in Wales[70]	Organizational level:	Public–private	and Promote
	Technology level:	Medium-tech	SMEs

The Welsh Development Agency (WDA) is the leading enabler of business support in Wales, working to stimulate more competitive businesses in vibrant communities. As a means of transforming both the economic and social well-being of Wales, the WDA places great importance on the development of a knowledge-based economy. The Agency proposes that to attain such an economy, everyone must be empowered with the ability to communicate and access information, freely and without barrier. Their goal is a society where all sectors public, private, education, health, individual citizens, and communities can interact with seamless ease—in short an Information Society.

ICT has been identified as crucial to achieving such a society, but it is not simply the existence of such technologies that is the key. It is the usage, understanding, skill levels, and supply of adequate support and infrastructure that will allow for an Information Society to develop and flourish effectively.

In 1999, the WDA published the Objective 1 Guide, through the Welsh Information Service (WIS). The purpose of the guide is to assist applicants and program managers of the 2000–2006 West Wales and the Valleys' Objective 1 Structural Fund Programme, to meet the cross-cutting objective of developing the Information Society. In particular, it offers advice and suggestions on how projects can exploit ICT to meet the aims of the Programme and bring to the region the benefits of the information and knowledge-based society, thereby supporting the development of the region and Wales as an attractive and competitive economy and cohesive society

Five goals put forth in this guide are as follows: (1) Increase awareness of the potentials offered by ICT; (2) Increase the number of people receiving ICT-related skills training and information; (3) Reduce the negative effects of peripherality; (4) Increase business competitiveness; and (5) Increase the range of public services provided through ICT to enhance business competitiveness. The guide prescribes five steps to accomplish these goals: (1) Provide financial support for SMEs; (2) Increase the birth rate of SMEs; (3) Develop competitive SMEs; (4) Promote entrepreneurship and adaptability; and (5) Provide an attractive environment for SMEs.

Real Practices—Case 32	Economic level:	Developed country	ICT to Support
Finnish National Fund for Research and Development (SITRA): Knowledge Economy Transformation in Finland[71]	Organizational level:	Public–private/ international	and Promote SMEs
	Technology level:	High-tech	

[70] Welsh Development Agency (WDA) (2002). Priority 1: Expanding and developing the SME base. In *Wales Information Society Objective 1 Guide*. Available: http://www.wis.org.uk/objective1guide/english/project/section4_pri1.htm.

[71] Routti, op. cit.

The Finnish National Fund for Research and Development (SITRA) is a policy think-tank and development institute that provides research information on Finnish society for the basis of decision-making, innovative operations to create new cooperative networks and models, training for decision makers and professionals in the field of corporate funding, corporate funding for startup technology companies, regional enterprises for technology transfer, and investments in international venture-capital funds concentrating on the high-tech field.[72]

During Finland's post-socialist economic crisis of the early 1990s, SITRA reported to the Parliament of Finland with an analysis of the driving forces and change processes of global and European scenarios to aid in economic recovery planning. Their forecasts were: (1) A possible market economy of regional coalitions ruled by prevailing democracy; (2) A possibility of multi-national corps of fierce competition, winning and losing; or (3) Possible conditions of factious alliances and turmoil. In the intervening decade, the outcome for global economy proved to be simultaneously all three.

Finland's revised policy formula, based on the possible futures forecast in SITRA's scenarios, included: public and private collaboration, emphasizing cooperation among companies and universities and research institutes; investment particularly in ICT[73]; knowledge-based, S&T excellence, to drive innovation and industrial practices; and, adoption of a free-market competitive economy.

By the end of the decade, the success of Finland's knowledge economy transformation was affirmed in some spectacular outcomes. According to the World Competitiveness Yearbook published by the Institute for Management Development (IMD), Finland rose from fifth to second in global competitiveness from 1999 to 2002.[74] Comparatively, the USA ranked first in all 4 years, and in 2002, Luxembourg, Netherlands, and Singapore came in sequence behind Finland, with Germany at a distant 15th, France 22nd, and Japan 30th. Data published by the World Economic Forum (WEF) shows that Finland now ranks second in growth competitiveness and microeconomic competitiveness, third in technology.[75] The Organisation for Economic Co-operation and Development (OECD) shows that Finland now paces Japan and the USA in R&D intensity. During 1988–2001, high-tech exports as a percentage of total exports increased for Finland from 5 to 25 %. Finland's R&D input as a percentage of GDP has risen from 1.5 to 3.6 % during 1985–2002, compared with a EU average around 2 %.[76] High-tech has completely changed Finland. Formerly, almost all exports were forest products. Now, more than 50 % of Finnish firms are in R&D co-ops.

---

[72]Finnish National Fund for Research and Development (SITRA) (2003). Available: http://www.sitra.fi/eng/index.asp.

[73]Telecommunications are the biggest area. In Finland, telecommunication is more valuable than roads.

[74]Institute for Management Development (IMD) (2003). World Competitiveness Yearbook (WCY). Available: http://www02.imd.ch/documents/wcy/content/pastranking.pdf.

[75]World Economic Forum (2003). *Competitiveness Profiles*. Available: http://www.weforum.org/site/knowledgenavigator.nsf/Content/KB+Country+Profiles.

[76]OECD, op. cit.

Dr. Jorga Routti, who was president of SITRA at the time the knowledge economy scenario planning was committed, offers this summary of Finland's success factors.[77]

> Science-driven academic research is vital to returns; scientists decide the basic research, but industrialists decide the applied R&D. One must have the best technology to remain global. Knowledge-based businesses must have their own intellectual property—otherwise they're just selling commodities. Competitive funding for R&D synergizes value; competitive funding is easier to reorient than institutional funding, one can also obtain many multiples of funding for a grand cause, more easily than sustained institutional funding. Researchers must convince themselves, then their peers, then funding authorities to obtain the funds. Institutionally, a deviation from planned use is an irregularity, but competitively it's creative, innovative, exploratory work. Creativity is essential; locked into old ways spells the end.

2.4 Thematic Areas for e-Development and Knowledge Economy Interventions

In this part we perform synthesis of the theoretical and prerequisite elements delineated at the beginning of this paper, respective of the pertinent dimensions addressed in the analysis, and borne out of the 32 case studies. Additional dimensions are also explored, and inferences are extracted and interpreted from the case findings.

We examine the critical factors for success and failure, and encapsulate a summary of best practices for each thematic area: using business incubators for new venture formation, and using ICT to support and promote SMEs. This is followed by an assessment of lessons learned and findings for policy and practice of e-development in the knowledge economy and the use of incubators for venture initiation and ICT to support and promote SMEs, from the perspective of both public and private sectors.

The paper concludes with recommendations for policy and practice of e-development in the knowledge economy and the use of incubators for venture initiation and ICT to support and promote SMEs, specifically in the thematic areas of skills for knowledge economy, science and technology, and innovation policy.

2.4.1 Dimensional Synthesis of Case Studies in e-Development and Knowledge Economy

In this section, we synthesize the fundamental concepts and instrumental methodologies of e-development and knowledge economy respective of the analytic dimensions of economic level, organizational level, and technology level, as exemplified in the 32 case studies. The additional dimensions of scale and time are also explored, and inferences extracted from the case findings are interpreted in terms of their similarities and differences.

---

[77] Routti, op. cit.

Table 2.5 Developing countries, by organizational level and technology level

Developing Countries	Low-Tech	Medium-Tech	High-Tech
For-Profit	Phone and fax extend the reach of a village sunglass maker.	Internet brings a global market to sandal makers at Ecosandals.com in Kenya.	VCs answer survey of new venture success factors.
Non-Profit	Indirect Internet access broadcasts on Radio Sagarmatha in Nepal.	Web mail services are delivered by Kabissa.org throughout Africa.	Quipunet connects Peruvians living around the world to home.
Public-Private / International	Development Gateway Foundation delivers information and knowledge sharing capability worldwide to reduce poverty and support sustainable development	UNECE promotes development in Eastern Europe, Baltic States & CIS. UK IDPM supports ICT in SED in developing countries.	Romania promotes competition in the ISP market.

Legend
■ Incubators
■ ICT

2.4.1.1 Three-Dimensional Summary of Cases

Tabulation of the analytic dimensions of economic level, organizational level, and technology level yields 27 points of conjunctional cells in this three-dimensional analysis. At least one case study has been selected to embody each conjunction in the matrices. Some cases, by their scope, span multiple cells.

Table 2.5 summarizes cases drawn from developing countries, arrayed by organizational level and technology level.

Table 2.6 summarizes cases drawn from emerging economies, arrayed by organizational level and technology level.

Table 2.7 summarizes cases drawn from developed Countries, arrayed by organizational level and technology level.

The case descriptions are color-coded to visually differentiate those cases pertaining primarily to using business incubators for new venture formation (coded in the tables in black text), and cases pertaining primarily to using ICT to support and promote SMEs (coded in the tables in blue text).

2.4.1.2 A Fourth Dimension: Scale

Synthesis and discussion of the fundamental concepts and instrumental methodologies of e-development and knowledge economy would not be complete without an evaluation of the analytic dimension of scale. In the context of the topic, scale refers

Table 2.6 Emerging economies, by organizational level and technology level

Emerging Economies	Low-Tech	Medium-Tech	High-Tech
For-Profit	Enterprise offers business incubator for women in Jordan	JTG provides venture capital incubator for early-stage IT firms in Jordan	Hsinchu Science-Based Industrial Park attracts expatriated engineers to return to Taiwan.
Non-Profit	Jhai Foundation helps farmers install pedal-powered Internet in Laos.	USAID Project Fabrykat 2000 designs a stronger manufacturing technology transfer system in Poland.	IBI helps build Silicon Valley business incubators in the U.S. for Korea, Scotland and India.
Public-Private / International	Development Gateway Foundation delivers information and knowledge sharing capability worldwide to reduce poverty and support sustainable development.	IADB promotes policy for sustainable development in Latin America and the Caribbean. Researchers write an academic prescription for virtual incubators in China.	TradenetSL provides virtual incubator services to export firms in Sri Lanka. Technical cooperation activities in Korea exhibit a steep upward trend.

Legend
■ Incubators
■ ICT

Table 2.7 Developed countries, by organizational level and technology level

Developed Countries	Low-Tech	Medium-Tech	High-Tech
For-Profit	PRSource.com reopens its online source for public relations services.	Microsoft sponsors incubator program for independent video game developers.	VCs answer survey of new venture success factors. MediMined wins NBIA award for technology incubator client (USA). NTT DoCoMo transforms multimedia market in Japan.
Non-Profit	FAME Renaissance incubates multimedia businesses in impoverished urban communities (USA).	ETHM launches entrepreneur training center for economic revitalization of distressed urban community (USA).	NBIA advances business incubation and entrepreneurship.
Public-Private / International	Telecottage brings ICT access for development in rural Australia	WDA promotes ICT for SMEs in Wales.	TEDCO fosters technology transfer. (USA). Arno valley promotes clusters of SME ICT producers in Italy. Finland experiences phenomenal success in ICT and the new economy.

Legend
■ Incubators
■ ICT

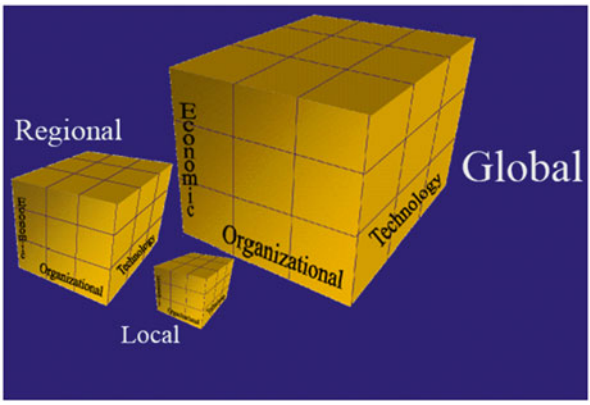

Fig. 2.18 The dimension of scale

to global, regional, and local levels of influence and operation, as modeled in Fig. 2.18. In the specific context of issues central to e-development, Carayannis and von Zedtwitz offer this perception:

> The global–local real-virtual incubator networks model may be particularly helpful in less developed economies, where incubators can help bridge knowledge, digital, socio-political and even cultural divides and help increase the availability, awareness, accessibility and affordability of financial, human, intellectual, and even social capital, the key ingredients of entrepreneurial success.

2.4.1.3 A Fifth Dimension: Time

Synthesis and discussion of the fundamental concepts and instrumental methodologies of e-development and knowledge economy would not be complete without an evaluation of the analytic dimension of time. In the context of the topic, scale refers to immediate, short-term, and long-term periods of performance, as pictured in Fig. 2.19. In the specific context of issues central to technology innovation, Hamel and Prahalad offer this insight:

> The future is now. The short term and the long term don't abut one another with a clear line of demarcation 5 years from now. The short term and long term are tightly intertwined. Although many of tomorrow's mega-opportunities are still in their infancy, companies around the world are, at this moment, competing for the privilege of parenting them.

2.4.1.4 Dimensional Synthesis of Cases: Economic Level—Similarities

The World is going through a dynamic era where a country's economy can transition quickly either upwards or downwards, and this trend has become increasingly more pronounced. At all levels of social and economic development, people seem eager to have access to ICT and all that it promises to offer. Everywhere in the

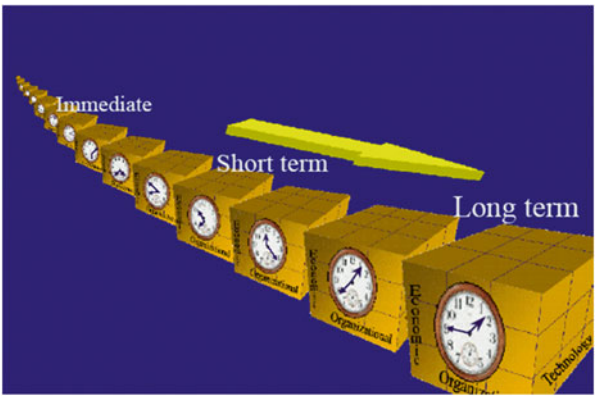

Fig. 2.19 The dimension of time

World, even across the most remote areas of the least developed countries, pioneers are delivering knowledge-based skills and resources. Where there is no infrastructure to support the newest and best, people are pooling their efforts, creativities, and meager means to extend the reach of the information age and share the enlightenment of connectivity. Where knowledge economy resources are more available, people are revising their ways of social transaction to leverage the improvements into even greater advantage.

At all levels of economic development, policy makers are deliberating or crafting improved regulatory environments to facilitate and promote the fruition of knowledge economy. Regulators are demonstrating a commendable understanding of the factors and conditions, and many are taking action to open up opportunities for their constituents. Organizations at all levels are engaging in directed strategic assistance to entrepreneurs and other stakeholders

2.4.1.5 Dimensional Synthesis of Cases: Economic Level—Differences

Clearly, the availability of existing resources and the leverage to build more are disparate between economic levels. In the developing countries, progress enacts on a small scale, in modest ventures by individuals or teams of relatively few actors. While involving more actors and commanding more attention, larger development projects in these nations tend to be exploratory, prescriptive, or still being studied. The greater resources available in emerging economies and developed countries permit positive actions earlier, which further stimulate economic growth. The healthier economic condition of many developed countries, particularly those of scant natural resources (lacking comparative advantage) is directly attributable to this upward spiral of technology investment, deployment, and adoption (competitive advantage).

When it comes to e-Development, developing countries are thinking about it at a policy level, but acting on it in fragmented cells of small enterprise. Emerging economies have made commitments and started to take concerted action at the policy level, including policy actions to foster the success and cross-pollination of small enterprise. Developed countries got that way—or sustain their prior development level—by having exercised their commitments and supporting actions from the outset of knowledge-based economy.

2.4.1.6 Dimensional Synthesis of Cases: Organizational Level—Similarities

The fundamental economic challenge facing all forms of social organization is at the very heart of economic discipline: ***The management and allocation of scarce resources.***

Regardless of organizational form or level, no single entity has everything that is wanted or needed to pursue that organization's mission to its fullest. For-profit enterprises must deliver financial returns to investors.

Nonprofit organizations must deliver targeted services to recipients. Public–private/International bodies must deliver an environment in which constituents grow and prosper. In all cases, the organizational mission must be accomplished before scarce resources are withdrawn or used up, but these same scare resources must be invested to build a for-profit enterprise up to a self-sustaining level; must be budgeted at a level adequate for a nonprofit organization to fulfill its mission competently; and must be committed by public–private and international institutions with prioritizations based on where the resources will do the greatest good for the most people, particularly in growing the resources to make more resources available. In all cases, collaboration and productivity can yield the sustaining level of results more economically—higher output per unit input: efficiency.

2.4.1.7 Dimensional Synthesis of Cases: Organizational Level—Differences

The motivation for operational emphasis is inherent to the organizational form and level. The primary purpose of for-profit enterprises is to increase shareholder wealth. Other social benefits are incidental not central, but most for-profits are in the business of selling social benefits (economic goods) rather than profiteering from causing harm. The primary purpose of nonprofit organization is to deliver specialized services. If this action creates or saves money, its incidental not central, but generally, nonprofits are not geared to be purposefully wasteful. The primary purpose of public–private/international institutions is to create and preserve environments in which the other organizations (and individuals) can function best to pursue their primary purposes without unreasonable restriction, but be constrained from engaging in harmful, wasteful, or unfair practices with respect to other organizations (and individuals).

2.4.1.8 Dimensional Synthesis of Cases: Technology Level—Similarities

Regardless of technology level, business incubators facilitate and enhance new venture formation, and improve the survivability and growth of the enterprise. From relatively low-tech office services or technical advisory assistance in low-tech business sectors, to high-tech mobile teleconferencing or research investigations into untested technology markets, the business incubator extends the reach and resources of the startup firm.

Regardless of technology level, ICT supports and promotes SME development. From relatively low-tech phone and fax lines, to high-tech portable information terminals or the collaboration of scientists, engineers, attorneys, and financial investors to patent and deploy a next-generation breakthrough, ICT enables the efficient transaction of knowledge exchange and gains in knowledge capital.

Competency of all organizational levels—in all economic environments—is elevated by technology.

The introduction of technology at any level, however modest, becomes a platform upon which the next technology can be adopted, and subsequent adoptions become increasingly easier for the user community

2.4.1.9 Dimensional Synthesis of Cases: Technology Level—Differences

The accessibility to technology is predominantly dictated by economic environment, by the very definition of economic levels for countries, although even the poorest countries have wealthy residents who have access to the highest technology, and the wealthiest countries have residents whose access to high-tech benefit is limited. Wherever this disparity occurs, it is often called the digital divide. While developed nations are investing hundreds of billions of dollars in a move to 3G networking with completely mobile data connectivity, the poorest developing countries are hand carrying e-mail copies to recipients on paper or diskette. 15 percent of the earth's population is providing nearly all of the world's technological innovations. Fifty-two percent is able to adopt these into production and consumption. Approximately one-third neither innovate nor adopt.

But as a technology matures, adoption leads to recovery of capital costs, prices go down and availability goes up, permitting diffusion into more economic sectors to accelerate.

2.4.1.10 Dimensional Synthesis of Cases: Scale—Similarities

The accessibility of ICT makes it increasingly easier for remote locales to participate in global commerce, diminishing geographic, political, and cultural boundaries. In the context of real and virtual networks of business incubators, the wide-range

access connectivity is called ***gloCal***.[78] This compares with the term "global village" in common parlance. ICT and network architecture is eminently scalable, provided that each node has connectivity to at least one other. As more nodes are added and interconnected, the exchange efficiency and transaction potential increase exponentially, amplifying the gloCal diminution of boundaries. At the highest level of proliferation, each new node is a network unto itself, all constituents of which have feasible access to all the constituents of all the other nodal networks. The number of connections on a network of membership networks or interactive groups is calculated by Reed's Law: $2N - N - 1$.

It genuinely is a World Wide Web. ICT and virtual incubator networks enable economic integration, which is a force for good. Globalization does not cause poverty. Globalization is the only feasible cure.[79]

2.4.1.11 Dimensional Synthesis of Cases: Scale—Differences

At all levels of scale—local, regional, and global—the economic benefits of ICT and business incubators have the same impact and availability. Access and implementation differences are a function of prevailing economic level and infrastructure. A wealthy person in a poor locale experiences connectivity challenges, which can be surmounted by supplemental technology, which perhaps that wealthy person can afford. Geographic remoteness is an obstacle whether the inhabitants are poor or wealthy, until infrastructure development brings connectivity to those who can afford it. These investments by those who can afford them create conditions that improve the affordability to everyone there.

2.4.1.12 Dimensional Synthesis of Cases: Time—Similarities

Economic development is an ongoing process. The drive for survival and ascent is both immediate and perpetual. Failure to act now, or at any time in the future will lead to social setbacks. Those who advance will pass those who do not compete. Economic vitality depends on active transactions. Knowledge economy moves faster than did the industrial economy, and ICT accelerates this trend.

2.4.1.13 Dimensional Synthesis of Cases: Time—Differences

Realistically, not everything can happen at once, particularly in the prudent management of scarce resources. Developing countries and policy makers need to target investments wisely, staged according to technical and financial feasibility. But the same planning and investment prudence pertains to every venture and organization.

---

[78] Carayannis and von Zedtwitz, op. cit.

[79] Crook, Clive (2001). Globalisation and its critics. *The Economist*, 2001, September 27.

A multi-billion-dollar program is of no less import to the stakeholders of a 3G ICT network than to the stakeholders of a transnational education program. Stakeholders are not just owners and investors, but also the policy makers, managers, technicians, workers, advisors, producers, consumers, users, and beneficiaries who are impacted by the outcomes of the program. Success is in everyone's interest. Failure is not without consequences. An immediate investment in e-development for knowledge economy can lead to short-term gains in knowledge capital, which in turn will leverage the capacity for an even greater long-term economic yield.

2.4.2 Critical Factors for Success and Failure of e-Development in the Knowledge Economy

2.4.2.1 Using Business Incubators for New Venture Formation: Success Factors and Best Practices

The following factors have been identified as the most critical to the successful and superior use of business incubators for new venture formation.

- The ability to evaluate and react to risk well
- The access to the right expert at the right time
- Protection of product
- To understand and exercise technology transfer privileges and intellectual property rights
- To foster actions oriented towards the production of academic spin-offs and entrepreneurial spin-offs
- To strengthen the education system
- To define programs for assistance and training in entrepreneurial functions
- Stimulation of existing market
- To promote venture-capital actions
- Having developed a good success formula, replicate it and franchise it

2.4.2.2 Using Business Incubators for New Venture Formation: Failure Factors

The following factors have been identified as having been most contributing to failure in the use of business incubators for new venture formation.

- Incapability risk
  - Entrepreneurial team lacking sufficient capability, principally in
  - Marketing
  - Input sourcing
  - Managerial competence

- Inexperience risk
  - Lack of familiarity with target market and relevant track record
- Product risk
  - Insufficient uniqueness of product/service relative to competitors (differentiation)
  - Inadequate product protection
  - Untapped market potential

2.4.2.3 Using ICT to Support and Promote SMEs: Success Factors and Best Practices

The following factors have been identified as the most critical to the successful and superior use of ICT to support and promote SMEs.

- To acquire technological knowledge from outside sources to supplement a narrow base
- The know-how and skills capacity (technical, managerial and developmental)
  - Both within the local ICT sector and among secondary ICT-users
- To start training in ICT applications and business skills at the earliest opportunity, and engage all stakeholders in continuing update training
- Open infrastructure development to competition
  - And use the access to market information to more precisely evaluate competitive offers
- To provide financial support for SMEs
- To increase the birth rate of SMEs
- To develop competitive SMEs
- To promote entrepreneurship and adaptability
- To engage in strategic community creation to advance and control the creative destruction of market infrastructure from multiple vantage points
- To use expanded access to market intelligence to predict market trends and make strategic plans to shift market emphasis accordingly
- To provide an attractive environment for SMEs
- For knowledge-based businesses to have their own intellectual property
  - Otherwise they're just selling commodities

2.4.2.4 Using ICT to Support and Promote SMEs: Failure Factors

The following factors have been identified as the most having been most contributing to failure in the use of ICT to support and promote SMEs.

- Studying the opportunity too long, thereby losing optimality or missing out entirely (paralysis by analysis)
- Not realizing that technology can be both overestimated and underestimated at the same time
- A general lack of financial, technical, and managerial resources
- Poor or unenforceable policy on ownership and transfer of knowledge and know-how (inadequate IPR protections)
- A corporate culture that is too rigid or risk averse
- Failure to recognize and actualize creative or innovative potentials

2.4.3 Lessons Learned and Findings for Policy and Practice of e-Development in the Knowledge Economy and the Use of Incubators for Venture Initiation and ICT to Support and Promote SMEs

> He who receives an idea from me receives instruction himself without lessening mine; as he who lights his taper at mine receives light without darkening me—Thomas Jefferson

Regardless of externalities, each organization seeks to sustain itself in competition and cooperation with other entities that depend on the same finite pool of resources. The fundamental challenge is the very heart of economic discipline: ***The management and allocation of scarce resources***.

The advantage of Knowledge Economy is that knowledge grows by sharing—donors do not forfeit what they know when passing knowledge to recipients, who in turn can share with others. The greatest phenomenon of knowledge-based economics is this multiplier effect: ***Sharing knowledge capital actually creates more of it.***

2.4.3.1 Lessons Learned and Findings: Public Policy

Governments have not surrendered their power to capitalism, even if the world's biggest companies are more powerful than many of the world's governments. Democracy is not a sham. People rule, not profits. Admittedly though, companies would run the world for profit if they could. What stops them is not governments, but markets. Economic parity arrives when technology allows people to pursue their own goals and they are given the liberty to do so. If technology can support trade across borders, and people choose to trade across borders, integration occurs. Because people have freely chosen it, the outcome is accepted, and because a free market is self-equilibrating, the trade precipitates economic benefits as well. Government must have a long-term commitment to building a market economy, and defending the mechanisms and protections in which a free market thrives.[80]

[80] Ibid.

2.4.3.2 Lessons Learned and Findings: Public Practice

Technology-enabled free trade is an economic equalizer. Governments have power, but they do not always exercise it wisely. They are unreliable servants of the public interest. But limited government is not worth buying Markets keep the spoils of corruption small. Government that intervenes vigorously is worth a great deal. Especially in developing countries with weak legal systems, taming capitalism by regulation or trade protection often proves such a hazardous endeavor.

Central strategic planning works best from a demand-side intervention, enacting and enforcing regulations that enable people to get what they want, while protecting society from harmful, wasteful, or unfair practices.

Historically what fails is central planning of supply-side regulations that specify what people may have, through prohibitions and licensing, by creating surpluses and shortages, or by setting quotas and prices to influence commerce and trade.

Distributed tactical planning works best under the control of the entrepreneurs, organizations, and actors operating in a free-market system. Government and NGOs function best when serving as facilitators and resources, not as managers and operators. If national governments or NGOs disable markets, the economic consequences can be dire, with direct spillover into political and social consequences. Governments must build transnational bridges of collaboration and cooperation, with immediate and long-term long commitment to building a market-oriented economy unimpeded by traditional boundaries.

2.4.3.3 Lessons Learned and Findings: Private Policy

Research and innovation must be managed today to secure sustainability for tomorrow. Open innovation is a policy of collaboration. Companies must manage intellectual property to manage research: they need to access external IP; they need to profit from internal IP. Researchers must be knowledge brokers as well as knowledge generators. Companies can profit from one another's IP. No one company has claim to all the smart people in a field. Competition and collaboration can and must co-exist. Open innovation is knowledge diffusion and recombination, producing the "seed corn" of tomorrow's breakthroughs. Researchers must recognize their own potential, and be able to articulate possibilities to a receptive management for further development.[81]

Science-driven academic research is vital to returns. Scientists decide the basic research; industrialists decide the applied R&D. Management culture must encourage risk-taking. Fear of failure suppresses creativity and innovation, which undermines competitiveness. Failure is a great educator. Institutionally, a deviation from plan is an irregularity, but competitively it is creative, innovative, exploratory work. Creativity is essential.[82]

---

[81] Chesbrough, op. cit.

[82] Routti, op. cit.

There is tremendous "white space" in market opportunities: new products, new processes, new markets, and new unknowns. Strategic community creation is a calculated alliance of many stakeholders to manage the white-space risk and facilitate adoption.

2.4.3.4 Lessons Learned and Findings: Private Practice

The priorities of new venture formation in the knowledge economy are: ICT and Internet access; linkages to investors and lenders; formation of lean management and advisory boards comprised of experienced individuals, competent in their fields of discipline and having as few members as needed to get the job done; and planning and securing facilities.

The priorities of e-development and sustained growth are: the ability to evaluate and react to risk well; protection of product; stimulation of existing market; the available population of skilled knowledge workers—whether centralized in a physical facility or linked via virtual organization.

All knowledge workers must have access to the Internet and competency in its use, ample training in computer literacy in addition to their specific technical expertise, and basic computer, math, and language skills. Firms must practice ongoing training to keep skills current; competitive advantage is volatile and requires constant reinforcement.

2.4.4 Recommendations for Policy and Practice of e-Development in the Knowledge Economy and the Use of Incubators for Venture Initiation and ICT to Support and Promote SMEs

2.4.4.1 Skills for Knowledge Economy

Knowledge Economy demands knowledge. Entrepreneurs need the knowledge to build a reliable infrastructure using incubators for new venture formation. New technology businesses need to move through the growth process rapidly and get their products to market before they run out of resources. Businesses need to use technology clusters to stimulate sustained innovation and growth.

Educators need the knowledge to educate in ICT and e-business, attaining digital literacy for all of society, and providing the knowledge to accelerate and embrace e-commerce. Everyone gains by providing electronic access to goods and information. Entrepreneurs need to understand the criticality of using ICT to support and promote SMEs, and using virtual incubators to enlarge and extend the accession and dissemination of knowledge.

Policy makers need the knowledge to accelerate and embrace e-government, providing electronic access to public services, enacting a regulatory environment conducive to the advancement of Science and Technology, and committing public policy to stimulate and assure innovation.

2.4.4.2 Science and Technology

The advancement of Science & Technology 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. The future of technology innovation depends on the building of strategic partnerships in S&T for economic development, and capacity building for competitiveness. This will be facilitated by the promotion of universal Internet access at affordable costs.

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.

2.4.4.3 Innovation Policy

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. The experience of post-socialist economies shows that a sole emphasis on networks may be misplaced and support to network organizers is equally or more important. The emphasis should be on functions and programs, not more organizations. Notwithstanding the spirit of enterprising individuals, the organizational and hence policy position may be more status quo than pro change. ICT networks are a vehicle to attain social capital, not social capital itself. Countries excluded from access to regional networks will fall behind.[83]

[83]Radosevic, Slavo (2000). Regional Innovation Systems in Central and Eastern Europe: Determinants, Organizers and Alignments. In *The emerging industrial architecture of the wider Europe, UK ESRC*. London: University College.

Chapter 3
Addressing the Impact of E-Development in the Knowledge Economy and Society: Outputs, Outcomes, and Impacts

Elias G. Carayannis

Abstract The analysis here is mainly concerned with e-Development applications that facilitate private sector development. The analysis will hinge on the main quantitative and qualitative data on ICT applications available from various sources, ranging from private sector to public sector in both developed and developing countries. The public sector's role as a facilitator in the promotion and adoption of information technologies is very important. While the private sector maintains the pivotal role in innovation and technology adoption, the public sector has the responsibility of designing and implementing reforms that create an environment conducive to economic growth. e-Development is a valuable tool to foster the interaction between the public and the private sector. Businesses are suppliers to, partners and customers of, and occasionally competitors with the government. A framework to monitor and evaluate e-Development will include a set of indicators which can be used to assess the benefits of implementing e-development projects. While a cost-benefit analysis is not the main focus of this study, the evaluation of e-Development hinges on comparing the costs and benefits of technology-based applications with traditional means of interaction. Both direct and indirect costs should be considered, where direct costs are represented by the resources needed by both the provider and user in implementing and using e-Development programs and systems. Technology brings unprecedented potential to make interactions between the public and the private sector easier, more efficient, and more transparent. Hence, these indicators become part of the evaluation to determine whether and how e-Development can support World Bank interventions in client countries and test the operational sustainability of e-Development-facilitated interventions.

E.G. Carayannis (✉)
Department of Information Systems and Technology Management, School of Business, George Washington University, Suite 515C, Funger Hall, 2201G Street NW, Washington, DC 20052, USA
e-mail: caraye@gwu.edu

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_3, © Springer Science+Business Media New York 2014

Keywords Cost-benefit analysis • e-Development • Developed countries • Developing countries • Information and communication technology (ICT) • Public sector • Private sector

e-Development is a set of tools, methodologies, and practices that leverages Information and Communication Technology (ICT) **to support and accelerate political and economic development**. From this perspective e-Development enables developing and transitioning countries to move toward a knowledge-based economy. In essence, e-Development is not about creating technology, but promoting and directing the best use of technology to achieve specific developmental results. International organizations—such as the United Nations (UN) system, the European Union (EU), and the World Bank Group—have been exploring the possibility of including ICT in their developmental interventions. At the same time, client countries are very eager to embrace new technologies capable of sustaining their transition process.

Recently, countries in the ECA region have shown particular interest in the use of Information and Communication Technology (ICT) to sustain their transformation process. The EU accession objectives encourage neighboring countries to reform not only their telecommunication infrastructure but also their general business environment and the regulatory framework supporting e-Applications (electronic signature, electronic transactions, etc.). This creates an overall favorable environment to the utilization of e-Applications in support of specific developmental objectives.

The business community is generally the first adopter and main driver of technology applications. In this context, this paper focuses on e-Development interventions targeted to the private sector and business community. The focus on private sector development does not undermine nor underestimate the value and relevance of e-Development applications targeted at civil society and government agencies, but helps define the scope of work.

Some open questions remain concerning the real impact of ICT applications in support of economic and social development. Despite the many efforts to use ICT for development, there is a lack of effective monitoring and evaluation (M&E) systems. The purpose of this note is to introduce M&E tools for a selected number of e-Development interventions so that program managers can utilize them for their current and future programs.

The study will aim to set an analytical framework to assess the feasibility, viability, and sustainability of e-Development interventions in transitioning and developing countries by:

(a) Identifying the **basic indicators** to determine the impact and validity of e-Development applications;
(b) Exploring the **viability** of e-Development applications aimed at private sector development through the analysis of costs and benefits associated with the deployment of technology;

(c) Assessing the practical **impact and implications** to target audiences of ICT applications in the private sector, by evaluating the improvements in the business environment and processes;
(d) Appraising the **sustainability** of ICT applications in support of private sector development in the ECA region.

3.1 Issues and Challenges in Measuring e-Development

This study is mainly concerned with e-Development applications that facilitate private sector development. The analysis will hinge on the main quantitative and qualitative data on ICT applications available from various sources, ranging from private sector to public sector in both developed and developing countries.

The public sector's role as a facilitator in the promotion and adoption of information technologies is very important. While the private sector maintains the pivotal role in innovation and technology adoption, the public sector has the responsibility of designing and implementing reforms that create an environment conducive to economic growth.

e-Development is a valuable tool to foster the interaction between the public and the private sector. Businesses are suppliers to, partners and customers of, and occasionally competitors with the government. In addition, businesses must comply with government regulations while maintaining these roles. The utilization of information technology to foster such a multifaceted interface holds the greatest promise for realizing new efficiencies, improving effectiveness and transparency.

A few main areas of e-Development have been identified in this paper for their relevance to private sector development priorities. Areas such as SME development, R&D promotion and innovation systems, and support of rural enterprises are representative of the wide range of issues related to private sector development, especially within the Knowledge Economy context.

Inherent advantages of e-Development

Comparing a technology based/online system with an offline system for private sector development is a very challenging exercise. Some key elements of e-Development solutions indicate a definite advantage of ICT applications for private sector development. A technology based system presents several intrinsic advantages by:

- **Reducing geographic constraints**: so that firms from all across the nation can run their business regardless of location;
- **Lowering interaction costs and time**: entrepreneurs will greatly benefit from e-Development systems that allow them interact more easily among each other and with the public administration, reducing costs and time;

(continued)

(continued)

- **Decreasing the impact of bureaucracy on private sector development**: e-Development brings about a more transparent and efficient way for the private sector to interact with the public administration;
- **Enhancing information sharing**: e-Development offers great opportunities for information and knowledge sharing. ICT becomes the privileged tool to create partnership and promote networking; and
- **Lowering barriers to entry**: by promoting transparency and creating room for cooperation, e-Development lowers barriers to entry in the economy, especially for SMEs. Thanks to e-Development, more entrepreneurs can take advantage of global knowledge and seek new opportunities.

Some of the major impediments for monitoring and evaluating e-Development projects are as follows:

- Lack of a reliable information infrastructure. Access and affordability of telecom infrastructure are crucial issues to sustain the viability of e-Development. From this perspective, the situation in the ECA region is uneven: some countries have high telephony penetration rates and technology levels, while others lag far behind. In this context, one of the working assumptions of this note is that entrepreneurs can have access to the needed infrastructure. Given the advances in technology, the options to overcome the "digital deficit" of entrepreneurs is increasing, for instance through the telecenters model, or through existing networks set up by Chambers of Commerce or other business associations.
- Scarcity of **sound evidence and exact quantitative data and statistics**. Yet, relevant and reliable qualitative facts and data mitigate and balance this challenge.
- Lack of an effective system to monetize the main benefits of increased efficiency and transparency brought about by e-Development. A cost-effectiveness analysis of e-Development may be rather straightforward for those applications that can draw on empirical data, such as reduction of administrative costs for registration procedures, increase in volume of online transactions for the business community, etc.
- Lack of Monitoring and Evaluating tools and frameworks for e-Development. In fact, although a generally positive evaluation of e-Applications within the business community of OECD countries exists—i.e., there is robust evidence on the viability of Business-to-Business (B2B) e-Procurement and e-Commerce in the most advanced economies and markets—there are only few tested models and frameworks to monitor and evaluate e-Development applications in transitioning and developing countries. Despite the growing inter-

est in ICT for development and the many initiatives undertaken to deploy technology for development, a unique and reliable framework to evaluate e-Development is still not available.

While a cost-benefit analysis is not the main focus of this study, the evaluation of e-Development hinges on **comparing the costs and benefits of technology based applications with traditional means of interaction**. Both direct and indirect costs should be considered, where direct costs are represented by the resources needed by both the provider and user in implementing and using e-Development programs and systems.

The cost associated with switching from an offline system to an e-enabled system is an important criterion. The related costs for training and development of human resources to manage the new e-enabled system need also be considered, as well as the direct costs incurred by the end users for using the systems. Entrepreneurs often question the effective delivery mechanism of public services. In most cases, firms may be willing to incur the one-time cost of setting up the infrastructure to adopt e-Systems that provide better service and ensure ease of operation. Such e-Enabled services mitigate administrative costs and hassles, such as physically going to the relevant public administration organization, as well as, in some cases, corruption and red tape.

The cost-effectiveness of e-Development interventions has to be carried out on a case by case and application specific basis, given the specificity of the costs and benefits involved that is not appropriate to generalize in this study. It is difficult to precisely measure the overall cost-benefit ratio of e-Development projects, given the problems in placing a monetary value on increased transparency and efficiency and its impact on private sector development. Notwithstanding the difficulty to properly estimate the benefits of e-Development interventions, particularly for its demand-driven and innovative nature, the approximation of the economic and social rate of return are expected to be high.

3.2 Analytical Framework and Indicators

A framework to monitor and evaluate e-Development will include a set of indicators which can be used to assess the benefits of implementing e-Development projects. Identifying indicators have proved to be challenging due to qualitative nature of the main benefits of e-Development, such as reducing red tape and corruption. It is easier to classify indicators that take into account the convenience of e-Development in terms of reduced time and costs on the interaction of the private and public sectors.

In general terms, the identification of indicators to evaluate e-Development should be based on the main advantages that are brought about by technology. For instance, in the case of reduction of geographic constraints, the monitoring efforts should focus on the ability of e-Development to foster wider participation and

improved access, bridge the rural/urban gap, and lower interaction costs and time. In this instance, an evaluation should hinge on a comparison of the ICT enabled system with the traditional means of delivery of the service. More challenging may be the evaluation of information sharing applications, due to the implicit difficulties in measuring knowledge sharing. In this case, it is possible to quantify the objective elements of the network: how many members, from where, what sort of information or knowledge is shared, and so on.

This section analyzes the potential of e-Development applications from various perspectives, trying to capture the essence of technology applications in promoting private sector activities and entrepreneurship. The section is conceptually divided in two parts. The first part describes applications to be implemented by the public sector to make it easier, cheaper, and faster for businesses to operate—these applications may be categorized under the general definition of e-Government for electronic delivery of services to the business sector. The second part focuses on e-Development as a tool for the **private sector to improve opportunities** and explore new venture. In this case, e-Development is a catalyst for knowledge creation, sharing, and use, fully designed and implemented by private sector.

3.2.1 e-Procurement

Public procurement should be competitive, to ensure the effective allocation of public funds in outsourcing goods or services. However, the public procurement process is often burdensome on both sides—supplier and buyer—given the many steps needed and the lengthy procedures. This is particularly the case in most developing countries since:

- Red tape and bureaucracy prevent the correct functioning of the procurement process;
- Only large companies are able to conduct business with the public sector by having greater capacity and possibilities than SMEs. In most cases, small enterprises and microenterprises are scattered across the country, with poor ability to track the opportunities offered by public procurement, which prevents effective competition from taking place;
- Entrepreneurs often lament a lack of overall transparency in the procurement process and allocation of public funds.

3.2.1.1 e-Procurement: Benefits

A technology-based procurement system for the public sector, or e-Procurement, can overcome most of these rigidities and provide ground for a more efficient and transparent system. In fact, e-Procurement applications can streamline the way tendering is being conducted, saving both time and cost for both government agencies

and entrepreneurs. e-Procurement is a more effective way to acquire goods and services from external suppliers and provides a platform for document interchange between suppliers and buyers. Besides increasing efficiency, the system greatly decreases level of corruption in government procurement operations.

For example, under the government e-Procurement system, companies need only to register a single time in the areas of their business (office furniture, construction services, IT consulting, etc.). Whenever a public agency needs to purchase goods or contract a service, the system automatically sends an e-mail to all the private companies registered in that selected area, minimizing response time and providing an equal opportunity for all the firms. The system also provides online all the information related to procurement operations. At the conclusion of the bidding process, the system provides the results: the list of participants, proposals, economic and technical scores, and, lastly, winners of the bid or contractors.

3.2.1.2 e-Procurement: Basic Indicators

To evaluate the effectiveness and the impact of e-Procurement systems, it is possible to rely on specific quantitative indicators that can be easily identified considering that e-Procurement applications allow to decrease the administrative burdens by dramatically **reducing the time** necessary to:

- Publish and advertise a tender for the public administration;
- Access tender information for entrepreneurs;
- Communicate "Detailed Bidding Documents" to all the parties that are interested in participating in the bidding process (by way of e-mail to all registered bidders);
- Process invitation for bids;
- Extend bid offers for entrepreneurs;
- Process requests of information on the tender offer;
- Process a request for quotes on the tender offer;
- Communicate either an approval or a rejection; and
- Process invoice payments.

In addition to removing administrative burdens, e-Procurement applications succeed in **cutting costs** for both buyers and suppliers, that can be measured by the savings in:

- Costs to manage the tender for the public administration:
  (a) Printing of documents;
  (b) Bid advertisement; and
  (c) Notification requirements.
- Costs associated to the preparation, submission, and follow-up of a bid for firms.

Mexico—Compranet, a national e-Procurement system

Compranet, the e-Procurement system of the Mexico's Federal Government,[1] was launched in April 2002. Compranet is a technology-enabled e-Procurement system set up by the Electronic Government Services Unit within the Mexican Ministry of the Controllership and Administrative Development (MCAD).

Reportedly, the system manages 80 % of all Federal Government acquisitions and has been largely successful in cutting administrative costs related to the whole procurement process. The following data reveal the great potential of e-Procurement systems:

- Administrative procurement costs and costs of procured items have been cut, with estimated savings around 20 %.
- Approximately 25,000 suppliers are using the system, and most state and municipality governments.
- Participation costs for businesses also appear to have fallen, and small/medium enterprises from outside the capital region have joined in the procurement process, although there has been no systematic analysis.

[1] Source: http://www.egov4dev.org/mexeproc.htm

e-Procurement is supported by information management systems that allow to **scale efficiency** in the relationship between the public administration and its suppliers. Such information management systems provide cheaper and more reliable ways to collect, use and share information about transaction history. Although efficiency is not easy to quantify, it is possible to measure how easier it becomes to:

- Screen bidders in the pre-qualification process;
- Collect and manage data and records related to bids, tenders and offers; and
- Monitor the post-tendering of public procurement.

Finally, e-Procurement applications allow for a **broader audience** of firms to participate in the public procurement processes. This increased participation can be measured by taking into account:

- Number of firms participating in public procurement;
- Number of suppliers interacting with the system by providing online self-registration for new vendors;
- Number of suppliers that submit bids online;
- Number of calls received per competition; and
- Reduction of support costs, because more complete product information available online to buyers should result in fewer inquiries for clarification.

UK—City of Leeds, e-Procurement for municipalities.

The City of Leeds launched in 2001 the Leeds Electronic Tendering System (LETS), as part of its e-Government strategy. The system, which took 9 months to become fully functional, allows both buyers and suppliers to perform tendering functions in an electronic environment.

The benefits realized as of September 2002 by the new system include:

- More than 20 % of contracts (£74 m worth out of £327 m of public procurement of the municipality of Leeds) were awarded through the new system and the amount is destined to grow in the next future;
- 2,170 organizations "self-registered" with LETS;
- 78,523 visits were recorded into the LETS system;
- 1,030 tenders were placed on the Web site;
- 2,405 documents were downloaded from the site;
- 124 electronic bids were received;
- 93 % of users rated the site as "good" or "very good".

3.2.2 e-Filing of Taxation

The efficiencies of the taxation process, collection of delinquent accounts, and tax enforcement and monitoring, are the major public sector concerns related to fiscal administration. The cumbersome tax filing processes, prolonged tax assessments as well as payment and refund procedures are the major business impediments associated with extra cost and time for private enterprises. The burden on firms in the ECA region may be exacerbated by continuous changes in fiscal and regulatory regime, making enterprises in the need of assessing relevant information and transparent legal information. Furthermore, the lack of centralized information systems and complicated regulation may lead to non-transparent environment conducive to shadow economy and corruption, hence preventing investment both local and foreign.

3.2.2.1 e-Filing of Taxation: Benefits

With the help of ICT, the government will be able not only to increase revenue collections and enhance process efficiencies but also to improve taxpayer services through the online system. The computerization of the tax administrations will allow the government to provide information about tax regulations in a timely manner and increase the speed and accuracy of the whole processing. Moreover, technology provides a system to better detect non-tax filers, reducing the administrative, processing, and transaction costs. These advantages for the public sector are mirrored by benefits for citizens and entrepreneurs alike. In fact, e-Development can revolutionize the interaction between tax authorities and taxpayers as well as the

exchange of data within government agencies, such as the ministry of finance and the land registry by electronic data exchange system.[1]

An e-Development tax system can be extremely beneficial to firms, since businesses will be able to access the relevant legal information anywhere anytime and get guidance and counseling for tax computation and filing. Economic advantages may hinge on the increased convenience and reduction of administrative costs—reduction of filing and processing time and potentially less costly accounting and fiscal management practice. Prospect foreign investors can also benefit: the online system will help them understand the country's complicated tax system, and provide details of corporate tax structures, laws, guidelines, procedures (i.e., payment and refund), and other relevant information.

3.2.2.2 e-Filing of Taxation: Basic Indicators

To evaluate the effectiveness and validity of e-Filing of taxation, the following quantitative indicators can be considered:

- Reduction of the number of days needed by the public administration to process a tax form;
- Reduction of the time spent by entrepreneurs in accessing tax information and obtaining the needed forms;
- Reduction of the time to prepare a tax form;
- Decrease in the costs for entrepreneurs to comply with tax requirement; and
- Decrease in the costs on the part of the administration for tax monitoring and tracking.

USA—Online Taxation

The US Internal Revenue Services (IRS) audited the benefits of e-Filing for tax-payers. Under the e-Filing system, electronically filed returns have higher accuracy rate of 99.5 %, compared to 82 % accuracy rate for the tax files mailed. The 18 % error rate for mailed returns is due primarily to manual data entry errors by IRS employees.

Taxpayers can receive their refund via direct deposit in only 10–14 days, compared to 8–12 weeks before. The IRS e-Filing system sends an acknowledgement record back to the filer for each return that is electronically processed. Mailed returns get no acknowledgement at all. Convenience is another definite advantage of the program, since the system is a "one-stop shop" tax filing. e-Filing allows taxpayers to file both their federal and state tax returns in one transmission.

(continued)

[1] The World Bank, PREM notes (2000) Computerizing tax and customs administrations. http://www1.worldbank.org/publicsector/tax/publications.html.

(continued)

Another example of e-Development system for taxation from the USA is the California Franchise Tax Board (CTFB). CTFB introduced e-Applications for tax collection and fiscal management with great results: 100,000 new non-filers were identified, resulting in $36 million in additional yearly tax revenues, while reducing erroneous contacts by more than half, with a dramatic cost reduction (each contact costs the Board an average US$ 7).

e-Filing systems dramatically reduce inconsistencies, erroneous contacts and faults that any taxpayers may incur by providing online support and assistance in filing tax returns. This **efficiency** gains can be evaluated through indicators that measure the efficiency gains by taking into account the increase in:

- Accuracy of tax return computation;
- Number of non-tax filers identified which will lead to an increase in tax revenues in short to medium-term;
- Amount of taxes collected through voluntary compliance encouraged by the more efficient system; and
- Number of registered businesses and individual tax payers.

UK—Direct benefits of e-Filing

In the UK, benefits from e-Filing processing have been estimated: the internal cost of processing a combined VAT return and check under the manual system is estimated to be £1.16, vs. £0.25 when the transaction is electronically processed a bank automatic teller (ATM) and less than £0.10 over the Internet.

3.2.3 e-Registration

Starting and running a business entails many administrative requirements. e-Development is a valuable tool to make registration a speedier, simpler, and more transparent process. From this perspective, e-Development is suitable not only for the registry of legal entities (corporate registry) but also for land registration to a Cadastre, registration of pledges to a mortgage registry, and registration of innovations to the patent bureau, just to mention few other examples. An e-Development application in these instances would facilitate the interaction between entrepreneurs and the public administration when formalizing property rights on physical and intellectual assets.

The following section presents cases and indicators relevant to corporate registration, selected as a representative example of the many operations that can be facilitated by e-Development. The indicators of this section may be easily extrapolated to evaluate other applications of electronic registration, especially those based on cost and time savings. Business registration and licensing procedures are often regarded as a major entry barrier in the ECA countries, since they put a heavy administrative burden on existing companies and would-be entrepreneurs.

While the number and type of licenses and requirements—ranging from fiscal and labor to health safety permits—depend on the commercial activities to be carried out, companies have to deal with the public administration in many ways in order to lawfully operate a business. The interaction between the public sector as service supplier, and the private sector as end user, can be dramatically improved by e-Development through the creation of one-stop shops for business registration and licensing, connecting the many public stakeholders to the convenience of entrepreneurs.

3.2.3.1 e-Registration: Benefits

One-stop shops for business registration provide a more efficient environment for entrepreneurship. An informative single point for registration facilitates the information gathering process on requisites and criteria for business registration, creates room for advisory and guidance services provision on the many requirements and processes, and ensures higher rates of accuracy. The deployment of ICT in these processes not only cuts red tape but creates a more transparent and accountable system by limiting the potential for corruption.

The public administration also gains from e-Registration systems, since it allows for a better allocation of public money through cheaper and faster processing, and more effective data collection and handling.

Electronic business registration is therefore a tool that can assist governments by:

- Providing a separate, dedicated one-stop shop where businesses can get access to information concerning business related matters;
- Providing linkages with other actors such as ministries, business advisory councils and export promotion offices through “one-stop shop” services;
- Providing efficient data warehousing and data mining; and
- Providing, subsequently, a reliable resource for all businesses.

3.2.3.2 e-Registration: Basic Indicators

Many indicators can be deployed to assess the impact of e-Registration on the business community and the public administration.

Technology facilitates the whole registration process by **decreasing time** consumption:

- For a business, to get all necessary documents and submit them;
- For the public administration, to process an application and grant a business license.

e-Registration also allows for **greater efficiencies by cutting costs to**:

- The administration, to disseminate information, manage the relationship with stakeholders, and process a business registration application;
- Entrepreneurs, in accessing vital information on requirements and procedures for business registration; and
- Companies, in complying with administrative requirements for business registration changes, license and permit renewals, etc.

Efficiency gains though e-Registration include:

- A simplification of the administrative requirements for start-up company; and
- A decrease in registration failure rate.

Canada—Electronic System for Business Registration

The Nova Scotia Business Registry (NSBR) relies on technology to allow entrepreneurs to register electronically in real-time, while offering companies online access to a wide range of services, including payroll deductions, corporate income tax, import/export accounts, and over 30 Nova Scotia business licenses and permits.

Through this one-stop shop Web site, over 60,000 companies interact with the Canadian government without geographical or time constraints. The system allows entrepreneurs to:

- Register with the Registry of Joint Stock Companies;
- Apply, pay for, and renew various licenses and permits;
- View and update general business and contact information;
- Register with the Workers' Compensation Board of Nova Scotia and obtain clearance letters;

Link to Canada Customs and Revenue Agency Services.

3.2.4 Dedicated Virtual Networks: Research and Development

Any national innovation system relies on the capacity of its main players (public sector, academia, research community, and the private sector) to carry out Research and Development (R&D) and commercialize new ideas. Traditional models of

support to R&D however present several challenges: the flow of information and knowledge sharing is fundamental to all R&D processes, and a lack of adequate systems of interaction may undermine the scalability of R&D activities and processes in bringing new ides to market.

In the ECA region, R&D entities fail to deliver on their potential due to fragmented network and communications systems. e-Development applications can help set up centers of excellence, dedicated R&D networks, and ICT models, to create an open system for recognizing, valuing, enriching, and sharing local and international knowledge, in parallel with activities building relevant human capacity, and establishing the right legal framework and system of incentives.

3.2.4.1 R&D Networks: Benefits

e-Development applications can provide R&D with appropriate platforms for knowledge sharing, through innovative forms of networks, efficient R&D cooperation schemes, and the creation of one-stop shops. This is mainly achieved by:

- Creating online fora for communication, consultation and coordination among all actors such as businesses, universities, governments (administrations), and research institutions;
- Facilitating the sharing of new methods, data, and best practices among researchers;
- Promoting innovative ideas and offering consulting services online to newly established business that lack either resources or networking abilities; and
- Improving cooperative research among researchers, government, businesses, and research institutions, thus facilitating links between theory and practice.

3.2.4.2 R&D Networks: Indicators

ICT can provide widespread and comprehensive dissemination of information through new information services—often Internet based—strongly articulated between suppliers and customers. New information services targeted at networks and clusters have a clear positive impact on developing countries, measurable in terms of:

- Number of participants in the network and their affiliation (i.e., public sector, private firm, academia, research institute, etc);
- Number of SMEs in the networks;
- Number of venture capitalists in the network;
- Number of partnerships and joint ventures created among firms, universities and research institutes;

- Number of research publications of the networks' members;
- Number of patents in the networks (or IPR in general);
- Worldwide linkages of the network and geographical reach (i.e., how many regions or countries are linked through the network);
- Number of innovation awards; and
- Type and number of services provided in the network.

EU—The Cordis Network

Cordis (http://www.cordis.lu/en/) is the European Community Research and Development Information Service designed to assist enterprises, and SMEs in particular, in technology transfer and innovation activities, through a wide range of services.

Within Cordis is the Network of **Innovation Relay Centers** (IRCs), established in 1995 and today a leading European network for the promotion of technology partnership and transfer between SMEs. Today, there are 68 Relay Centers in the EU, Iceland, Norway, Switzerland, Israel, Cyprus, and 10 ECA countries (Bulgaria, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, and Slovenia).

IRCs cooperate with local agents and organizations such as Chambers of Commerce, Regional Development Agencies, universities, research institutes and industrial centers, helping them to transfer their results to the industry. A top priority for the IRC Network is to continually extend its contact base and strengthen the links between companies in all participating countries. To achieve this goal, the network has developed a portfolio of information services that responds to the specific needs of the IRC client companies in each region.

The IRC Internet site is a virtual meeting point for all members of the IRC Network and their partners. The site is divided into a public and private area. In the public area are the directory, all IRC members and their partner organizations, as well as hyperlinks with their own Web sites, and publications and success stories of recent technology transfer projects. The private area is a form where IRC members run their business.

In 5 years IRCs have assisted over 5,000 technology transfer negotiations, and helped 65,000 client companies to meet their technology needs and exploit their research results.

3.2.5 Virtual Business Incubator (VBI)

Business incubation is a dynamic process of business enterprise development, in which young firms are nurtured and helped to survive/grow in the early stages, when they are most vulnerable to market shocks and skills shortages. The goal of business incubators is to produce healthy firms that sustain growth and employment, strengthen the economy, and commercialize new technologies.

Business incubators provide firms with hands-on management assistance, guidance on how to access financing, various business and technical support services, logistics, and access to equipment. e-Development applications can be deployed to create VBI and reinvent the traditional business incubation model, overcoming the problem of location and access to incubation services for companies located across the country.

3.2.5.1 Virtual Business Incubator: Benefits

A VBI provides effective ICT-enabled business online counseling, matchmaking and project management services to the semi-virtual and virtual tenants, i.e., start-up companies that are linked on the VBI through technology networks. Online counseling enhances the effectiveness of traditional tailor-made training, mentoring, and consulting services as entrepreneurs achieve a better preliminary understanding of the subject. Additionally, a VBI provides online business advice on developing business ideas, formulating effective business plans, providing business and strategic planning, proactive support, marketing and sales advice as well as management support and training.

3.2.5.2 Virtual Business Incubator: Indicators

The contribution of a VBI to the economic business environment of a country could be assessed via the following indicators:

- New jobs generated by hosted companies;
- Survival rate of the companies created through the VBI;
- Number of services provided to entrepreneurs through VBI;
- Number of companies hosted;
- Length of tenancy within a VBI;
- Reach of the VBI: origin of hosted companies (i.e., local, regional, national, and international);
- Internationalization of hosted companies, i.e., how many hosted companies manage to explore new markets;
- Number of partnerships created through the virtual model;
- Number of economic sectors covered by the VBI; and
- Number of business plans drawn up and received.

UK—The Cambridge Virtual Incubator

The Cambridge Virtual Incubator (CVI, http://www.cambridgevirtualincubator.com/index.html) is a partnership of the Cambridge Enterprise Services, Cambridge University Entrepreneurship Center, Business Link Services in Cambridgeshire, and St. Johns Innovation Center in Cambridge. These 4 organizations run extensive networks of people, training courses, and in-house advisers.

A start-up company based in Cambridgeshire which intends to use the virtual incubator must provide information to all 4 partners, and is guided through a highly structured incubation process, with all partners sharing information and managing the virtual network. The company can learn how to run its business, receiving the right support at each critical phase in its development, and develop computer databases which inform its employees, partners, suppliers, potential markets about its development, operation working, and offerings of goods and services.

CVI offers a wide range of services to the virtual tenants, from funding and start-up advice and business development, to design, technology and innovation services and marketing.

3.2.6 e-Marketplace

The lack of appropriate means of interaction often prevents firms, especially SMEs, in the ECA region from taking advantages of opportunities of global markets. In fact, most SMEs remain confined in local markets despite their potential and competitive advantage at international level—such advantage is most often a combination of high R&D potential, lower costs and quality levels. Globalization and technology improvements establish new trends of increased competition and shorter product life cycles that force companies to examine and experiment with new inter-enterprise opportunities, enabled by Internet technologies, which can deliver higher efficiency, lower costs, and greater business agility.

The e-Marketplace makes it possible to conduct various business transactions besides purchasing, such as: (1) checking prices and stock availability; (2) invoicing and chasing order; (3) managing catalog content; (4) converting product information into a common language; (5) supporting the trading processes, i.e., shipping, online auctions, tendering, etc.

Since 1999, an estimated 800 to 1,200 online marketplaces have been established. The table below highlights e-Marketplaces proliferating in every major vertical industry, including energy, chemicals, high-tech, bandwidth, maintenance and financial services, as well as many niche markets. Some industries, such as construction and metals, have 150 or more such marketplaces.

Value of B2B Global e-Commerce Sales By Industry 2000–2005, in US$ billion

	2000	2001	2002	2003	2004	2005
Food (processing and service)	5.5	16	67	148	240	380
Manufacturing supplies/general	4.9	18	55	130	220	290
Utilities	3.5	20	50	100	150	170
Chemicals	3.2	18	35	70	130	155
Retail	2.5	11	32	68	100	145
Automotive	2.8	12	33	68	106	130
Information technology/electronic components	9.9	18	43	65	87	125
Paper	1.2	5	16	45	75	90
Building/construction	4	12	24	37	58	70
Agriculture	3.8	11	17	41	50	60
Metals/mining	5.5	13	20	28	36	45
Plastics	0.9	7	19	27	39	45
Shipping/freight/logistics	4.2	11	18	28	36	40
Health	3.5	12	17	25	34	40
Telecoms equipment and services	0.2	4	12	17	27	35
Printing	0.1	4	8	14	19	22
Aerospace	0.2	3	6	10	12	14
Textiles	0.1	3	5	7	9	10
Other	8.8	16	26	40	46	50
TOTAL	64.8	214	503	968	1,474	1,916

Source: Euromonitor, 2000

3.2.6.1 e-Marketplace: Benefits

e-Marketplaces can help integrate enterprises in ECA countries into the international value chains, by improving their ability to interact at regional and international level. The forum to foster development of the financial and private sector in the ECA region may take different shapes. There are valid examples of positive experiences in terms of structure and content that can be leveraged to ensure viability to the proposed forum. The rationale behind the creation of an e-Marketplace is to virtually allow companies in ECA to get integrated into the international markets and switch from the traditional one-to-one system to the many-to-many of a virtual market.

The potential of e-Marketplaces for the companies in ECA is to generate significant network effects—largely through broadening buyer-supplier relationships—so that each new participant adds value to all other participants, generating increasing returns to scale. e-Marketplaces are crucial for the development of the private sector in the global markets, allowing to overcome industry and sector specific inefficiencies by:

- Building a solid community of trading partners;
- Providing rich content to trading partners;

- Delivering a collaborative infrastructure for product design, supply-chain planning and fulfillment processes;
- Aggregating industry-wide product information into a common classification and catalog structure;
- Enabling online sourcing, negotiations and other trading processes to enhance buyer and supplier interactions and overall market transparency; and
- Creating an online community for publishing and exchanging industry news, information, and events.

3.2.6.2 e-Marketplace: Basic Indicators

Evaluation of e-Marketplaces has primarily focused on the growth of the volume and value of goods traded online. Boston Consulting Group estimated that B2B e-Commerce would account for $2.8 trillion by 2003. Forrester Research offers a similar forecast, with B2B e-Commerce market deemed to reach $3 trillion by 2003. The Gartner Group actually foresees the worldwide B2B market to increase from $145 billion in 1999 to $7.29 trillion in 2004.

The sustainability and viability of e-Marketplaces can be evaluated on qualitative indicators, such as:

- Number of companies trading on the marketplace and their geographical locations;
- Growth in number of companies joining the marketplace;
- Growth in volume of the trade;
- Growth in value of transactions;
- Growth percentage of total sales conducted online by the companies;
- Savings in overhead costs by companies after switching to the e-Supply Chain Management;
- Growth in productivity of the companies;
- Improvement in delivery time of goods and services;
- Reduction in the level of unproductive inventory;
- Number of new markets created; and
- Consumer satisfaction—rating of feedback.

USA—BuyUSA.com

BuyUSA.com (www.buyusa.com) is an e-Marketplace that brings buyers and sellers together in a powerful online environment backed by the US Department of Commerce. Its mission is to bring suppliers of US products and services together with companies outside the USA, and provides both groups the services they need to conduct successful business worldwide.

(continued)

(continued)

The US Commercial Service of the US Department of Commerce of more than 1,800 trade experts in 105 US Export Assistance Centers and 151 posts located in US Embassies, Consulates, and Trade Centers in 84 countries are connected to assist companies navigate the complex international trade process. Currently, about 3,000 US companies registered with their 6,000 product and service listings on the e-Marketplace. About 2,000 of them offer the link to the company Web site, and about 300 product/service information is on the online catalog.

BuyUSA.com combines the power of the Internet with the extensive network of US Commercial Service specialists. It provides even the smallest US businesses with the means to export their products and services. Its dynamic program maximizes SMEs' international exposure, while minimizing the cost of finding reputable international partners and reducing the time needed to enter international markets. BuyUSA.com provides assistance to help US exporters move into international markets. Furthermore, US supplier member benefits include: instant access to qualified international trade partners; online brochure and link to the company website; international market research on countries and industries worldwide; customized international trade counseling (identify the best export markets, develop the market entry as well as marketing and selling strategies); and exposure at global promotional events.

BuyUSA.com also helps international (non-US) companies to conduct business with Reputable US suppliers. Its personalized consulting services, sales offers from US suppliers, business matchmaking services, market research, and other dynamic features are available to assist international companies in finding the right US business partners and procuring quality goods and services.

3.3 Closing Remarks

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. Many international donor organizations have launched programs to leverage ICT for development. Notwithstanding the increasing interest in e-Development, a framework to properly assess the electronic means of value creation is still missing. Most e-Development interventions are carried out without a systematic framework to test the viability of technology applications in developing countries. Such shortcoming may undermine the deployment of technology in many client countries ultimately slowing the transition process toward a Knowledge Based Economy.

More specifically, the lack of a framework to evaluate the efficiency gains of technology has prevented e-Development from becoming an integral part of the World Bank efforts. This study has provided a framework that can be used to preliminarily assess the viability of e-Development applications. The indicators allow to test the impact on both the provider and the users of electronic means of value creation. The list of indicators may not be exhaustive, but definitely represents a first step in the challenge of developing a tool to monitor and evaluate ICT applications in transitioning economies.

This paper provides examples of e-Development applications that can be implemented both by the public sector and the private sector to streamline bureaucratic procedures and foster entrepreneurship. The examples and indicators reported in the paper are meant as a tool for Task Team Leaders, to assess the opportunity and viability of e-Development in supporting the development objectives of their client countries. The cases provided below highlights in particular the cost reduction, efficiency, and transparency gains that can be achieved through e-Development. Hence, these indicators become part of the evaluation to determine whether and how e-Development can support World Bank interventions in client countries, and test the operational sustainability of e-Development facilitated interventions.

Part II
Cyber-Democracy

David F.J. Campbell

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 emerging 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 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. 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 coevolution 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 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) 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 (for example 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 by-passes 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 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 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 DFJ, Carayannis EG (2013) Epistemic governance in higher education. Quality enhancement of universities for development. SpringerBriefs in business. Springer, New York, NY (http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6)

Carayannis EG, Campbell DFJ (2009) "Mode 3" and "Quadruple helix": Toward a 21st century fractal innovation ecosystem. Int J Technol Manage 46 (3/4): 201–34 (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 EG, Campbell DFJ (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 transdisciplinary analysis of sustainable development and social ecology. Int J Soc Ecol Sustain Dev 1(1): 41–69 (http://www.igi-global.com/bookstore/article.aspx?titleid=41959)

Carayannis EG, Campbell DFJ (2012) Mode 3 knowledge production in quadruple helix innovation systems. 21st-century democracy, innovation, and entrepreneurship for development. SpringerBriefs in Business, vol 7. Springer, New York, NY (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 SA (1990) The science of cybernetics and the cybernetics of science. Cybern Syst 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. John Wiley New York, NY

Chapter 4
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

David F.J. Campbell and Elias G. Carayannis

Abstract The analytical research question of this contribution is twofold: (1) to compare the quality of democracy of the USA internationally and to "assess" (evaluate) American democracy, whereas assessing (evaluation) in this scenario refers to putting results of the comparative rating in the form of propositions (theses) for further discussions; (2) this same frame of reference is also being used to compare the quality of democracy in Austria internationally, and to propose more specifically a whole set of reform measures for further improvement of the quality of Austrian democracy in the nearer future. 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 dimensions of freedom, equality, control, and sustainable development, for explaining and comparing democracy and quality of democracy. Put in summary, we may conclude: the comparative strengths of the quality of democracy in the USA 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 USA. The comparative weakness of the quality of American democracy lies in the dimension of equality, most importantly

D.F.J. Campbell (✉)
Faculty for Interdisciplinary Studies, Institute of Science Communication and Higher Education Research, University of Klagenfurt, Schottenfeldgasse 29, Klagenfurt 1070, Austria

Department of Political Science, University of Vienna, Universitätsstrasse 7/2, Vienna 1010, Austria
e-mail: david.campbell@uni-klu.ac.at; david.campbell@univie.ac.at

E.G. Carayannis
Department of Information Systems and Technology Management, School of Business, George Washington University, Suite 515C, Funger Hall, 2201G Street NW, Washington, DC 20052, USA
e-mail: caraye@gwu.edu

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_4,

income equality. Income inequality defines and represents a major challenge and concern for democracy in the USA. In the "epilogue" to our analysis, we engage in reflecting on *Cyberdemocracy* and possible ramifications for *Knowledge Democracy*. We present a few propositions for further discussion and discourse.

Keywords Austria • Basic quadruple-dimensional structure of quality of democracy • Democracy • Cyberdemocracy • International comparison of OECD countries • Knowledge democracy • Quality of democracy • The USA

4.1 Introduction: Research Question for the Analysis and Presentation of the Research Design

This contribution focuses on analyzing the quality of democracy of the USA and of Austria by using a comparative approach.[1] Even though comparisons are not the only possible or legitimate method of research, this analysis is based on the opinion that comparisons provide crucial analytical perspectives and learning opportunities. Following is the proposition, put directly forward: *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, for example 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 contribution is twofold: (1) to compare the quality of democracy of the USA internationally and to "assess" (evaluate) American democracy, whereas assessing (evaluation) in this scenario refers to putting results of the comparative rating in the form of propositions (theses) for further discussions; (2) this same frame of reference will also be used to compare the quality of democracy in Austria internationally, and to propose more specifically a whole set of reform measures for further improvement of the quality of Austrian democracy in the nearer future (see also Campbell 2012).[2] In this line of thinking the USA and Austria mark the two more specific country cases that will be compared in the analysis presented here (they represent the "poles" of our thinking). The national political systems of the USA and Austria are the main references in this case in which American (US) and Austrian democracy and quality of democracy are to be compared with all other member countries of the OECD (Organization for Economic Co-Operation and

[1] In the Epilogue, we also present some ideas and tentative propositions on the relationship of quality of democracy with (or to) cyberdemocracy. This should help extending the perspective of democracy particularly in context of knowledge democracy.

[2] This also explains the empirical focus of the used literature on Austria, as is being documented in the reference list at the end. Regarding the USA, we do not engage in developing recommendations for reform measures in the context of the analysis presented here.

Development) and of the European Union (EU15, EU27) for a comparative analysis, thus leading to a country-based comparison of democratic quality.[3] Supranational aggregations (like of the whole European Union at EU level) or transnational aggregations (global level) shall not be dealt with. The OECD primarily comprises of the systems of Western Europe (EU as well as Non-EU), North America (the USA and Canada), Japan, Australia, and New Zealand. Outside these regions, Israel, Mexico, and Chile are part of the OECD, which highlights the global expansion 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 Carayannis and Campbell 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."[4] 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 to be made with the USA and with Austria, in order to carry out a "fair" comparison. For a comparison of the quality of democracy of the USA and of Austria, the "comparative benchmark" must be of the highest possible standard, in order to submit theses questioning about which other democracies can have a positive effect on the American as well as Austrian quality of democracy. *Concerning quality of democracy*, *what can the USA learn from other democracies*? This same question may be also applied to Austrian democracy.

The emphasis on the American and Austrian quality of democracy in comparison with OECD will not lie on a time-series pattern; instead it will focus on an indicator-specific system using empirical information available from the latest available year (mostly 2010, referring to data publicly accessible as of early 2012). A broad spectrum of indicators will be considered for this purpose, 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 of the USA and of Austria in a broader time perspective. As of January 2012, the OECD has over 34 member countries. *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

[3] Most, however not all, member countries of the EU are also member countries to the OECD.

[4] Quotes from original sources in German were translated into English by the authors of this analysis (DC and EC).

an expansion of the group of countries to "OECD plus EU27." These additional countries are Bulgaria, Latvia, Lithuania, Malta, Romania, and Cyprus. In total, the quality of democracy of the USA and of Austria will be put into comparison with 39 other countries (including the USA and Austria, 40 countries).

Not only 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; Schmidt 2010). Metaphorically, based on these (partly contradictory) different theories, democracy theory could also be constructed as a *meta-theory*. Theoretically, democracy can be understood as *multi-paradigmatic*, meaning that there is not only one (dominant) paradigm for democracy (on paradigms, see also Kuhn 1962). 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 for example Campbell and Barth 2009; Lauth et al. 2000; Lauth 2004, 2010, 2011; Munck 2009; 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). The field of the quality of democracy is no longer a vague one, especially not for OECD-countries.

The further structure of this contribution is divided into the following four sections: in Sect. 4.2, different conceptualizations of democracy are presented, followed by the concrete empirical comparison of the quality of democracy in the USA and in Austria in Sect. 4.3. In the conclusion (Sect. 4.4), an attempt to assess the quality of democracy in the USA and in Austria is being made and opportunities for improving the Austrian democratic quality are presented for further discussion. In the final Sect. 4.5 (epilogue), we also explore possible ramifications of "cyberdemocracy" (*Cyberdemocracy*) for democracy, quality of democracy and knowledge democracy.

4.2 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*

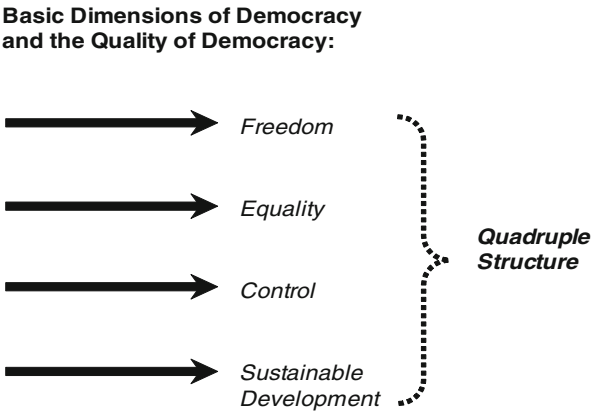

Fig. 4.1 The basic quadruple-dimensional structure of democracy and the quality of democracy. *Source*: Authors' own conceptualization and visualization based on Campbell (2008, p. 32; 2012, p. 296), Campbell and Carayannis (2013a), and for the dimension of "control" on Lauth (2004, pp. 32–101)

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 Fig. 4.1).[5] Lauth (2004: 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 theory development.

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).

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 for example: 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

[5] These dimensions we want to interpret as "Basic Dimensions" of democracy and of the quality of democracy.

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, for example, 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).

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. 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 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, multiparty 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. 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").[6] 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

[6] In the Figs. 4.2 and 4.3, 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.

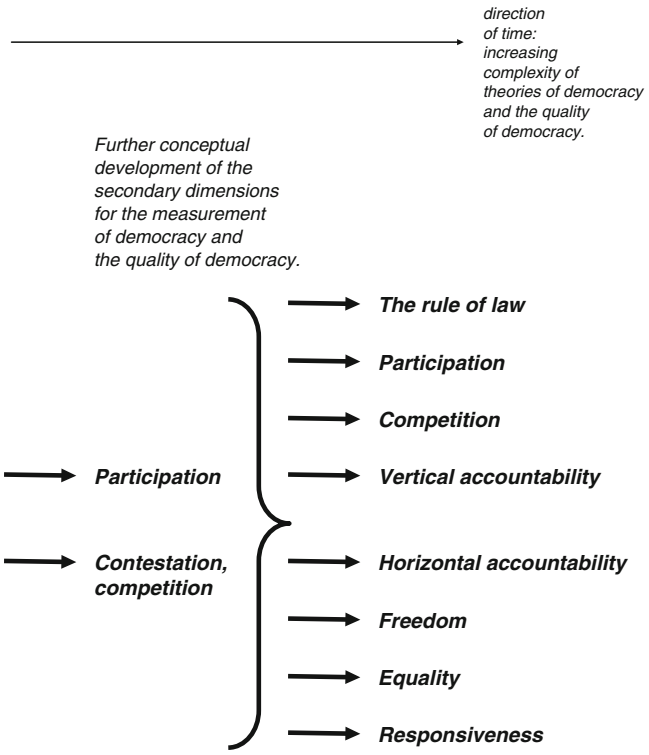

Fig. 4.2 Dimensions (Secondary Dimensions) for the Measurement of Democracy and the Quality of Democracy (Part A). *Source*: Authors' own conceptualization and visualization based on Dahl (1971), Diamond and Morlino (2004, pp. 20–31; 2005) and Campbell (2008, p. 26)

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*;[7] (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 regards 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 Figs. 4.2 and 4.3).

[7] See Schmitter (2004).

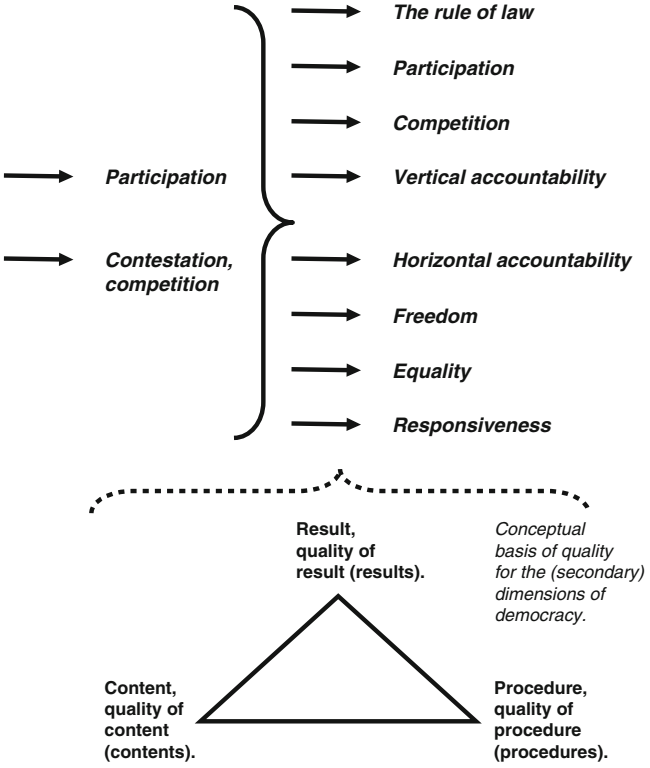

Fig. 4.3 Dimensions (secondary dimensions) for the measurement of democracy and the quality of democracy (part B). *Source*: Authors' own conceptualization and visualization based on Dahl (1971), Diamond and Morlino (2004, pp. 20–31; 2005) and Campbell (2008, p. 26)

"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.[8] Democracies themselves are subject to further 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.*

[8] 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 %.

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 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; O'Donnell 2004b). 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).[9] 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*.[10] 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. 4.1). 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

[9] For a comprehensive Web site address for all *Human Development Reports* that is publicly accessible for free downloads, see: http://hdr.undp.org/en/reports/global/hdr2011/.

[10] For a systematic attempt of empirical assessment on possible linkages between democracy and development, see Przeworski et al. (2003).

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" as well as "civil society." *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 socio-ecological 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 proposed a* "*Quadruple-dimensional structure*" *of four different* "*basic dimensions*" *of democracy that are being called freedom*, *equality*, *control*, *and sustainable development* (Fig. 4.1 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* emphasizes 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 4.4 introduces a possible visualization from a helix perspective for a theoretical framing of democracy.

As already mentioned, equality is often associated closer with left-wing political positions and freedom with right-wing positions. *A measure of performance of political and non-political 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

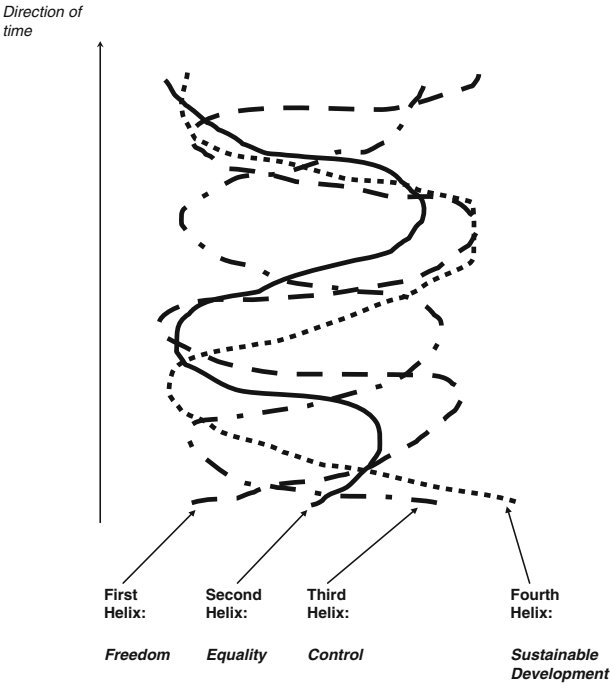

Fig. 4.4 The quadruple helix structure of the basic dimensions of democracy and the quality of democracy. *Source*: Authors' own conceptualization based on Etzkowitz and Leydesdorff (2000, p. 112), Carayannis and Campbell (2012, p. 14), Danilda et al. (2009), Campbell (2008, p. 32) and for the dimension of "control" on Lauth (2004, pp. 32–101)

the "Democracy Ranking" for the quality of democracy is: "Quality of Democracy = (freedom & other characteristics of the political system) & (performance on the nonpolitical dimensions)." *This 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).

Several global initiatives already exist that commit themselves to regular empirical democracy measurement.[11] The works of Freedom House (see, for example Gastil 1993) and of the Democracy Ranking shall be elaborated in more detail during the analysis of the quality of democracy in the USA and in Austria. Other initiatives (without claiming entirety) include: Vanhanen's Index of Democracy[12]

[11] It cannot be convincingly argued that there are no data or indicators for a comparative measurement of democracy (at least in the recent years). Of course there can and should be discussions about the quality of these data and their cross-references to theory of democracy.

[12] See: http://www.prio.no/CSCW/Datasets/Governance/Vanhanens-index-of-democracy.

(Vanhanen 2000); Polity IV[13]; Democracy Index[14] (EIU 2010); and the Democracy Barometer[15] (Bühlmann et al. 2011) (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."[16] 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. 4.1).

The *International Institute for Democracy and Electoral Assistance* (International IDEA),[17] established in Stockholm, Sweden, dedicated itself to the approach of the *Democratic Audit* by assessing the quality of democracy. 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) 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" (see also Beetham 2004). Beetham has been successively involved in various Democratic Audit Processes in the UK (see, for example 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, though excluding Austria, Germany, and Switzerland.[18]

To summarize the current stance of research and studies regarding the quality of democracy of 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).[19] In an exclusive chapter contribution

[13] See: http://www.systemicpeace.org/polity/polity4.htm.

[14] See: http://www.eiu.com/public/topical_report.aspx?campaignid=demo2010.

[15] See: http://www.democracybarometer.org/.

[16] 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.

[17] See: http://www.idea.int/.

[18] For an overview see: http://www.idea.int/sod/worldwide/reports.cfm.

[19] This book already can be downloaded for free as a whole and complete PDF from the Web. Visit the following links at: http://www.oegpw.at/sek_agora/publikationen.htm and http://www.ssoar.info/ssoar/View/?resid=12473.

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*")[20] on one hand and power-balancing structures ("*Macht-ausbalancierenden Strukturen*")[21] on the other (Campbell 2002, p. 19). Later studies have already started preferring a comparative approach (see Beck et al. 2003; Fröschl et al. 2008; Barth 2010; Barth 2011).

4.3 The Quality of Democracy in the USA and in Austria in a Comparative Perspective with the OECD Countries (EU27): A Comparative Empirical View of the American and Austrian Democracy Relating to the Dimensions of Freedom, Equality, Control, and Sustainable Development

The following session validates the quality of democracy in the USA and in Austria through empirical indicators by providing a comparative approach and analysis in order to create a platform to discuss the propositions for assessing and analyzing American and Austrian quality of democracy (as is being attempted finally in Sect. 4.4). 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.[22] 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 re-scaled on a rating spectrum from 0–100, in which "0" indicates*

[20] "*Grundrechte*" here may be interpreted as *human rights* as they are being proposed by Guillermo O'Donnell (2004a, pp. 12, 47).

[21] 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).

[22] Partially, in the following Tables 4.1 and 4.2, we had to estimate, to which calendar year a specific index year referred to.

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 forty-country-sample here*).[23] Results of that re-scaling are being represented in Table 4.1. Data in Table 4.2 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.[24] Mean values in Tables 4.1 and 4.2 are not weighted by population. The comparison is based on a total of eleven indicators, in which the majority (more or less) fits nicely or at least convincingly into the four identified (basic) dimensions of democracy (see Fig. 4.1 in Sect. 4.2). 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 4.1 and 4.2, 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 USA itself (see also the discussion by Pickel and Pickel 2006, p. 221; see further more Rosenberger and Seeber 2008). 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

[23] For the process of re-scaling 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.

[24] Therefore, put in contrast, a comparison of the indicators in Table 4.1 and 4.2 should allow for a better and more nuanced interpretation of the different countries and their quality of democracy (OECD, EU27).

Table 4.1 Quality of democracy of the 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
Czech Republic	95.00	95.00	90.00	85.33	79.35	97.38	49.41	91.64	80.39	55.42	40.24
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
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
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

(continued)

Table 4.1 (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)
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		
USA	95.00	93.33	92.22	94.30	86.74	81.41	76.32	96.46	89.45	74.70	74.39
UK	100.00	95.00	90.00	90.30	87.33	85.73	81.70	91.43	90.48	68.67	71.95
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 re-scaling 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 (per indicator)

Table 4.2 Quality of democracy of the 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
Czech Republic	84.62	87.50	82.69	45.50	32.41	92.25	24.19	68.03	52.23	28.85	26.87
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
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
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

(continued)

Table 4.2 (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)
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		
USA	84.62	83.33	86.54	78.83	56.60	44.96	64.52	86.48	74.30	59.62	68.66
UK	100.00	87.50	82.69	63.96	58.54	57.75	72.58	67.21	76.82	50.00	65.67
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 re-scaling based on original sources (see text for source citation)
Scale range 0–100, 0=lowest empirical value, 100=highest empirical value (per indicator)

equality, the *Social and Welfare Statistics* of the OECD (2011) are used for reference. Concerning 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).[25] The Gini coefficient is also known as the "Gini index."

3. *The dimension of control*: The *Corruption Perceptions Index* (CPI) is used in this regard, which is published yearly by Transparency International (TI 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 the Tables 4.1 and 4.2, 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*.[26] 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 non-citizens 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.

[25] Concerning the Gini coefficient (re-scaled as income equality) in the Tables 4.1 and 4.2, 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."

[26] See also: http://www.democracyranking.org/en/.

4.4 Conclusion: Comparative Assessment and Evaluation of the Quality of Democracy in the USA and in Austria and Measures for Improving the Quality of Democracy of Austria

The following central research question coined the analytical procedure of this analysis: *to compare the quality of democracy in the USA and in Austria internationally and to* "*assess*" (*evaluate*) *it*. For this particular reason, American (US) and Austrian democracy were put in reference to the OECD countries (EU27) with 2010 as the main year in focus. Theoretically, four basic dimensions (freedom, equality, control, and sustainable development) were derived conceptually and allocated to eleven empirical indicators. Tables 4.1 and 4.2 (in Sect. 4.3) present the relevant empirical evidence. The main concern is to provide an attempt for the evaluation of American and Austrian quality of democracy through a comparative perspective. In the following, we provide a first assessment for the quality of democracy in the USA, based on the empirical data that is strictly and consistently comparative in nature and character, and put forward first propositions. Afterwards, we focus in greater detail on the quality of Austrian democracy, and engage there also in the formulation of recommendations for democracy quality improvement. *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*.

For the comparative assessment of the quality of democracy in the USA we can put forward the following tentative propositions. The USA ranks highest on the Human Development Index (dimension of sustainable development) and on political rights, economic freedom, civil liberties, and freedom of press (all dimension of freedom).[27] Concerning the dimension of equality, the scoring of the USA is not that good anymore. With regard to gender equality, the USA positions itself slightly above OECD average, but concerning income equality, the USA performs clearly below OECD average. Concerning the perceived corruption, we asserted that this indicator could be assigned to the dimension of control. In reference to the Corruption Perceptions Index, the USA scores higher (meaning to have less perceived corruption) than the OECD average, but behind several of the more developed OECD countries.[28] Concerning the data of the Democracy Ranking 2011 (dimension of sustainable development), the USA performs clearly above the OECD average.[29] On the Migrant Integration Policy Index (MIPEX), the USA also scores above OECD average.[30] *Put in summary*, *we may conclude*: *the comparative strengths of the quality of democracy in the USA focus on the dimension of freedom*

[27] Interestingly, with regard to political rights and civil liberties, the USA ranks behind Austria.

[28] Levels of corruption are being perceived to be higher in the USA than in Austria.

[29] In the Democracy Ranking 2011, Austrian democracy scores higher than the USA.

[30] On migrant integration policy, Austria scores dramatically lower than the USA

and on the dimension of sustainable development. Further containment of corruption marks potentially a sensitive area and issue for the USA. The comparative weakness of the quality of American democracy lies in the dimension of equality, most importantly income equality. Income inequality defines and represents a major challenge and concern for democracy in the USA.

In the following, we want to focus now in more detail 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 thesis formulation:

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) show a problematic positioning. Austria's comprehensive rank in the MIPEX is only 26 (out of 33),[31] and in the category of access to citizenship, Austria ranks only 30 (out of 33)[32] (see Tables 4.1 and 4.2). 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 non-citizens (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*.[33]

[31] Here are behind Austria only Bulgaria, Lithuania, Japan, Malta, the Slovak Republic, Cyprus, and Latvia.

[32] Here, only Lithuania, Estonia, and Latvia perform poorer than Austria.

[33] "*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, 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*.[34] *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*.[35] Reforms in citizenship law in other European countries (like Germany), in the recent years, did not enter into Austrian politics and were not taken up by the Austrian mainstream political discourses.[36]

Finally, some possibilities for the betterment of the Austrian quality of democracy are to be sketched and presented for 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

[34] Here we can quote 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).

[35] 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; Pelinka and Rosenberger 2003).

[36] 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 completely be ruled out that the pure *jus sanguinis* design will finally be challenged legally at a "constitutional court" (nationally, supranationally, or even internationally).

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.[37]
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 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,[38] 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 of these provinces (Campbell 2007, pp. 392–393). 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*"); 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).[39]
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

[37] On the financing of politics and political parties in Austria see, for example: Sickinger (2009).

[38] For an analysis of the Austrian federal governments in these years, see: Wineroither (2009).

[39] 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*").

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); a populist abuse of certain political themes (for example 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. 250,000 signatures would probably not suffice. 640,000 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).

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*.[40] For this purpose, for example the procedure of IDEA could be used and applied (see IDEA 2008; Beetham 1994). However, it would also be possible to hybridize or pool different procedures.[41]

4.5 Epilogue on Cyberdemocracy

The research question of our analysis focused on conceptualizing and measuring quality of democracy. In particular, we put the two country-based democracies of the USA and of Austria into comparison. The OECD countries served as the general frame of reference for context. *Now*, *how does Cyberdemocracy 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 cyberdemocracy 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 cyberdemocracy 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 cyberdemocracy:

[40] 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.

[41] For the interesting example of a democratic audit in Costa Rica, see Cullell (2004).

1. *Cyberdemocracy 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 shifts have 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. *Cyberdemocracy*, *in fact*, *amplifies and accelerates the momentum of knowledge democracy. Cyberdemocracy 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 cyberdemocracy and knowledge democracy overlap in a conceptual understanding, but also in the manifestation of empirical phenomena. Cyberdemocracy expresses a particular vision, for how knowledge democracy may evolve further in certain and particular characteristics. *IT-based public spaces in cyberdemocracy operate nationally and subnationally. Cyberdemocracy*, *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 cyberdemocracy are certainly multilevel (global, national, and subnational). The global and transnational aspect of public space in cyberdemocracy 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. *Cyberdemocracy and Governance*: Cyberdemocracy 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 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; 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*.

3. *Cyberdemocracy*, *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. 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. *Cyberdemocracy and the New Rights and New Freedoms*: Cyberdemocracy 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 of restricting* (*technically possible*) *monitoring activities of democratic governments. Democratic governments*, *in fact*, *should impose on themselves also self-restrictions in that respect*.[42] 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 cyberdemocracy 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*.

References

Barth TD (2010) Konzeption, Messung und Rating der Demokratiequalität. Brasilien, Südafrika, Australien und die Russische Föderation 1997–2006. VDM Verlag Dr. Müller, Saarbrücken

Barth TD (2011) Die 20 besten Demokratien der Welt. Freiheit – Gleichheit – Demokratiequalität auf einen Blick. Books on Demand, Norderstedt

Beck E, Robert A, Schaller C (2003) Zur Qualität der britischen und österreichischen Demokratie. Böhlau, Vienna

[42] A related question here is: Is it proper for democratic governments to "spy" against each other?

Beetham D (1994) Key principles and indices for a democratic audit, 25–43. In: Beetham D (ed) Defining and measuring democracy. Sage, London

Beetham D (2004) Freedom as the foundation. J Democr 15(4):61–75

Beetham D, Byrne I, Ngan P, Weir S (2002) Democracy under blair. A democratic audit of the United Kingdom. Politico's Publishing, London

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. doi:10.1057/eps.2011.46 (http://www.palgrave-journals.com/eps/journal/vaop/ncurrent/abs/eps201146a.html)

Campbell DFJ (2002) Zur Demokratiequalität von politischem Wechsel, Wettbewerb und politischem System in Österreich, 19–46. In: Campbell DFJ, Schaller C (eds) Demokratiequalität in Österreich. Leske + Budrich, Opladen, http://www.oegpw.at/sek_agora/publikationen.htm and http://www.ssoar.info/ssoar/View/?resid=12473

Campbell DFJ (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 DFJ (2008) The basic concept for the democracy ranking of the quality of democracy. Democracy Ranking, Vienna, http://www.democracyranking.org/downloads/basic_concept_democracy_ranking_2008_A4.pdf

Campbell DFJ (2011) Key findings (summary abstract) of the democracy ranking 2011 and of the democracy improvement ranking 2011. Democracy Ranking, Vienna, http://www.democracyranking.org/downloads/Key-findings_Democracy-Ranking_2011_en-A4.pdf

Campbell DFJ (2012) Die österreichische Demokratiequalität in Perspektive [The quality of democracy in austria in perspective]. In: Helms L, Wineroither DM (eds) Die österreichische Demokratie im Vergleich [Austrian democracy in comparison]. Baden-Baden, Nomos, pp 293–315

Campbell DFJ, Liebhart K, Martinsen R, Schaller C, Schedler A (eds) (1996) Die Qualität der österreichischen Demokratie. Versuche einer Annäherung. Manz, Vienna

Campbell DFJ, Schaller C (eds) (2002) Demokratiequalität in Österreich. Zustand und Entwicklungsperspektiven. Leske + Budrich, Opladen, http://www.oegpw.at/sek_agora/publikationen.htm und http://www.ssoar.info/ssoar/View/?resid=12473

Campbell DFJ, Sükösd M (eds) (2002) Feasibility study for a quality ranking of democracies. Global Democracy Award, Vienna, http://www.democracyranking.org/downloads/feasibility_study-a4-e-01.pdf

Campbell DFJ, Barth TD (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 DFJ, Carayannis EG (2013a) Quality of democracy and innovation, 1527–1534. In: Carayannis EG, Dubina IN, Seel N, Campbell DFJ, Uzunidis D (eds) Encyclopedia of creativity, invention, innovation and entrepreneurship. Springer, New York, NY, http://link.springer.com/referenceworkentry/10.1007%2F978-1-4614-3858-8_509#

Campbell DFJ, Carayannis EG (2013b) Epistemic governance in higher education. Quality enhancement of universities for development (SpringerBriefs in Business). Springer, New York, NY, http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6

Carayannis EG, Campbell DFJ (2009) "Mode 3" and "Quadruple Helix": toward a 21st century fractal innovation ecosystem. Int J Technol Manage 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 EG, Campbell DFJ (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. Int J Soc Ecol Sustain Dev 1(1):41–69, http://www.igi-global.com/bookstore/article.aspx?titleid=41959

Carayannis EG, Campbell DFJ (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. J Knowl Econ 2(3):327–372, http://www.springerlink.com/content/d1lr223321305579/

Carayannis EG, Campbell DFJ (2012) Mode 3 knowledge production in quadruple helix innovation systems. 21st-Century democracy, innovation, and entrepreneurship for development. SpringerBriefs in Business, vol 7. Springer, New York, NY, 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 EG, Barth TD, Campbell DFJ (2012) The quintuple helix innovation model: global warming as a challenge and driver for innovation. J Innov Entrep 1(1):1–12, http://www.innovation-entrepreneurship.com/content/pdf/2192-5372-1-2.pdf

Cullell JV (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: O'Donnell G, Cullell JV, Iazzetta OM (eds) The quality of democracy. Theory and applications. University of Notre Dame Press, Notre Dame, IN, pp 93–162

Cunningham F (2002) Theories of democracy. Routledge, London

Dahl RA (1971) Polyarchy. Participation and opposition. Yale University Press, New Haven, CT

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. Democracy ranking, Vienna, http://www.democracyranking.org/en/ranking.htm

Diamond L, Morlino L (2004) The quality of democracy. An overview. J Democr 15(4):20–31

Diamond L, Morlino L (2005) Assessing the quality of democracy. The Johns Hopkins University Press, Baltimore, MD

Downs A (1957) An economic theory of democracy. Addison-Wesley, Boston, MA

EIU/Economist Intelligence Unit (2010) Democracy index 2010. Democracy in retreat. Economist Intelligence Unit, London, 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. Res Policy 29:109–123

Freedom House (2011a) Freedom in the world 2011. Methodology. Freedom House, Washington, DC, http://www.freedomhouse.org/template.cfm?page=351&ana_page=379&year=2011

Freedom House (2011b) Freedom in the world – population trends. Freedom House, Washington, DC, http://www.freedomhouse.org/images/File/fiw/historical/PopulationTrendsFIW1980-2011.pdf

Freedom House (2011c) Freedom in the world aggregate and subcategory scores. DC. Freedom House, Washington, DC, http://www.freedomhouse.org/images/File/fiw/historical/AggregateScores_FIW2003-2011.xls

Freedom House (2011d) Freedom of the press. Country reports, 2011th edn. Freedom House, Washington, DC, 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. Studienverlag (Transaction Publishers), Innsbruck

Gastil RD (1993) The Comparative Survey of Freedom: Experiences and Suggestions, 21–46. In: Inkeles A (ed) On measuring democracy. Studienverlag (Transaction Publishers), New Brunswick, NJ

Harding S, Phillips D, Fogarty M (1986) Contrasting values in Western Europe. Unity, diversity and change. Studies in the contemporary values of modern society. MacMillan, London

Hausmann R, Tyson LD, Zahidi S (2011) The global gender gap report 2011. World Economic Forum, Genf, http://www3.weforum.org/docs/WEF_GenderGap_Report_2011.pdf

Held D (2006) Models of democracy. Stanford University Press, Stanford

Helms L (2007) Die Institutionalisierung der liberalen Demokratie. Deutschland im internationalen Vergleich. Campus, Frankfurt
Heritage Foundation (2011) 2011 Index of economic freedom. Ranking the countries. The Heritage Foundation, Washington, DC, http://www.heritage.org/index/pdf/2011/Index2011_Ranking.pdf
Huddleston T, Niessen J, Chaoimh EN, White E (eds) (2011) Migrant integration policy index III. British Council and Migration Policy Group, Brüssel, http://www.mipex.eu/sites/default/files/downloads/migrant_integration_policy_index_mipexiii_2011.pdf
IDEA/International Institute for Democracy and Electoral Assistance (Beetham D, Carvalho E, Landman T, Weir S) (2008) Assessing the quality of democracy. A practical guide. International IDEA, Stockholm, http://www.idea.int/publications/aqd/index.cfm
IMF/International Monetary Fund (2011) World economic outlook, April 2011. International Monetary Fund, Washington, DC, http://www.imf.org/external/pubs/ft/weo/2011/01/pdf/text.pdf
Kuhn TS (1962) The structure of scientific revolutions. The University of Chicago Press, Chicago, IL
Lauth H-J (2004) Demokratie und Demokratiemessung. Eine konzeptionelle Grundlegung für den interkulturellen Vergleich. VS Verlag für Sozialwissenschaften, Wiesbaden
Lauth H-J (2010) Möglichkeiten und Grenzen der Demokratiemessung. Zeitschr Staats Europawissensch 8(4):498–529
Lauth H-J (2011) Qualitative Ansätze der Demokratiemessung. Zeitschr Staats Europawissensch 9(1):49–77
Lauth H-J, Pickel G, Welzel C (eds) (2000) Demokratiemessung. Westdeutscher Verlag, Wiesbaden
Marshall TH (1964) Class, citizenship, and social development. Essays. Doubleday, Garden City, NY
Müller WC, Strøm K (2000) Conclusion: coalition governance in Western Europe. In: Müller WC, Strøm K (eds) Coalition governments in Western Europe. Oxford University Press, Oxford, pp 559–592
Munck GL (2009) Measuring democracy. The Johns Hopkins University Press, Baltimore, MD
O'Donnell G (2004a) Human development, human rights, and democracy. In: O'Donnell G, Cullell JV, Iazzetta OM (eds) The quality of democracy. Theory and applications. University of Notre Dame Press, Notre Dame, IN, pp 9–92
O'Donnell G (2004b) Why the rule of law matters. J Democr 15(4):32–46
OECD (2011) OECD stat extracts. Social and welfare statistics. OECD, Paris, http://stats.oecd.org/index.aspx
Pelinka A (2008) Democratisation and de-democratisation in Austria. In: Fröschl E et al (eds) Democratisation and de-democratisation in Europe? Austria, Britain, Italy, and the Czech Republic – a comparison. Studienverlag (Transaction Publishers), Innsbruck, pp 21–36
Pelinka A, Rosenberger S (2003) Österreichische Politik. Grundlagen, Strukturen, Trends. Facultas WUV, Vienna
Pickel S, Pickel G (2006) Politische Kultur- und Demokratieforschung. Grundbegriffe, Theorien, Methoden. VS Verlag für Sozialwissenschaften, Wiesbaden
Poier K (2001) Minderheitenfreundliches Mehrheitswahlrecht. Rechts- und politikwissenschaftliche Überlegungen zu Fragen des Wahlrechts und der Wahlsystematik. Böhlau, Vienna
Przeworski A, Alvarez ME, Cheibub JA, Limongi F (2003) Democracy and development. Political institutions and well-being in the world, 1950–1990. Cambridge University Press, Cambridge
Rosenberger S (ed) (2010) Asylpolitik in Österreich. Unterbringung im Fokus. Facultas, Vienna
Rosenberger S, Seeber G (2008) Wählen. Facultas WUV (UTB), Vienna
Schmidt MG (2010) Demokratietheorien. VS Verlag für Sozialwissenschaften, Wiesbaden
Schmitter PC (2004) The ambiguous virtues of accountability. J Democr 15(4):47–60
Sickinger H (2009) Politikfinanzierung in Österreich. Czernin, Vienna
Sodaro MJ (2004) Comparative politics. A global introduction. Mc Graw Hill, Boston, MA
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. TI, Berlin, http://www.transparency.org/content/download/61964/992803

Umpleby SA (1990) The science of cybernetics and the cybernetics of science. Cybernet Syst 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 University Press, Oxford, http://hdr.undp.org/en/reports/global/hdr2000/

UNDP/United Nations Development Program (2011) Human development report. Sustainability and equity: a better future for all. UNDP, New York, http://hdr.undp.org/en/media/HDR_2011_EN_Complete.pdf

Valchars G (2006) Defizitäre Demokratie. Staatsbürgerschaft und Wahlrecht im Einwanderungsland Österreich. Braumüller, Vienna

Vanhanen T (2000) A new dataset for measuring democracy, 1810–1998. J Peace Res 37(2): 251–265

Wiener N (1948) Cybernetics or control and communication in the animal and the machine. John Wiley & Sons Inc., New York

Wineroither DM (2009) Kanzlermacht – Machtkanzler? Die Regierung Schüssel in historischen und internationalen Vergleich. LIT-Verlag, Vienna

Winiwarter V, Knoll M (2007) Umweltgeschichte. Böhlau, Cologne

Chapter 5
The Effects of Cyberdemocracy on the Middle East: Egypt and Iran

Robert F. Xavier and David F.J. Campbell

Abstract The effects of the internet have proved to be a major catalyst for democratic reform in the Middle East. These changes have been mainly attributed to social media networks and the free flow of information through the internet. The purpose of this analysis is to uncover the degree and impact these movements have played in the Middle East through cyberdemocracy. The Arab Spring has shown how cyberdemocracy in action can make a major impact in changing regimes. Egypt and Iran serve as the primary case studies to understand these changes while formulating our analytical view for the future of these states. The analysis aims to uncover the underlying realities of the dynamics of events and trends that led to this monumental change in the course of history for the region.

Keywords Arab spring • Green revolution • Cyberdemocracy • Democracy • Facebook • Twitter • LinkedIn • YouTube • Google • Iranian Revolutionary Guard Corps • Blogosphere • Digital divide • Social media • Muslim brotherhood • Islamist

R.F. Xavier
Middle East Analyst
e-mail: rfrxavier@gmail.com

D.F.J. Campbell (✉)
Faculty for Interdisciplinary Studies, Institute of Science Communication and Higher Education Research, University of Klagenfurt, Schottenfeldgasse 29, Klagenfurt 1070, Austria

Department of Political Science, University of Vienna, Universitätsstrasse 7/2, Vienna 1010, Austria
e-mail: david.campbell@uni-klu.ac.at; david.campbell@univie.ac.at

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_5,

5.1 Introduction

"If you want to liberate a society, just give them the Internet." Wael Ghonim, a Google executive turned online revolutionary made this statement as his conclusion on the effectiveness of the new dimension of cyberdemocracy in the Arab Spring. Cyberdemocracy engages citizens to take part in the democratic process through various outlets now readily available in the digital age. This dynamic process has never been more fascinating to see than through its revolutionary dimension in facilitating change in the developing world. This dimension of cyberdemocracy is believed to have toppled authoritarian regimes of states who are still struggling to find a resolution to the change it delivered as it continues to unfold. One region deeply impacted by the use of cyberdemocracy is the Middle East.

The Middle East, a region where change and reform was once seen as an impossibility, is today redefining itself as a place for new possibilities. On December 17, 2010 Tunisian vegetable vendor, Mohamed Bouazizi, immolated himself publicly in desperation to voice his opposition to the mistreatment and harassment he faced by local officials in Tunisia. His self-immolation is credited as the catalyst for the Arab Spring. The term Arab Spring defines a period of widespread revolutionary demonstrations against several governments in the Arab world from late-2010 to 2011. The onset of this event inspired protests in Jordan, Egypt, Algeria, Libya, Bahrain, Morocco, and Syria. Protesters utilized the internet to voice their discontent and organize against their governments by taking to the streets. Although technology served as a key facilitator for coordinating massive protests in the region, it was not the sole reason for the Arab Spring. There were already several issues that enabled the Arab Spring to flourish. Whether it be socioeconomic disparities, lack of participation in government, or nepotism in the political and economic sphere, the deteriorated state of affairs in these countries left many with no choice but to call for change.

We must note, the Arab Spring was not an isolated incident in the region. Similar demonstrations took place before the Arab Spring in Iran following the disputed presidential election of President Mahmoud Ahmadinejad in 2009. Iranians protested in opposition to what was viewed as a highly contested election, where the reformist candidate, Mir-Hossein Mousavi, conceded the election to the incumbent Ahmadinejad. Like the Arab Spring, voters utilized the internet and social media to make their demands heard and to expose their discontent to the rest of the world. Unlike the Arab Spring, the "Green Revolution" was not successful. The impact of these events in Iran played an important role in providing a framework for the Arab Spring.

The Arab Spring showed the revolutionary dimension of cyberdemocracy by reinforcing the view that technology acts as a facilitator for change in society, but technology is not the defining factor for the change witnessed. It provided a means to an end by connecting an audience to a cause of fostering change. This chapter aims to uncover and understand the role cyberdemocracy played during the Arab Spring.

We aim to uncover the tools used during the Arab spring and identify the role these tools continue to play in the Middle East. We will also analyze the attempts these regimes made to curb the use of these tools to maintain power. Egypt and Iran will serve as a basis for comparison and contrast as case studies to understand the effects of these movements respectively. Finally, this chapter will develop conclusions on the outcomes of these events while processing the challenges facings these countries and the future role of cyberdemocracy.

5.2 The Tools of Cyberdemocracy in the Middle East

Several tools were identified as the key contributor to the success of the Arab Spring. Social media was one source of technology widely accredited as the most influential tool for bringing the masses together to call for change. Social media sites like Facebook, Twitter, YouTube, and blogs were used constantly during this time. In order to understand this trend, we must uncover the demographics of these web users in the region, and relate this trend to the development of web usage in the Middle East.

5.2.1 Demographics and the Digital Divide

Internet usage in the Middle East has increased rapidly since the turn of the twenty-first century. Four years before the Arab Spring, Albrecht Hofheinz of the University of Oslo, wrote about developing trends emerging as a result of expanded internet usage in the region. Although he claimed the usage of the internet did not result in the overthrow of autocratic regimes in 2005, his research uncovered the tools that served as a foundation leading to the Arab Spring (Hofheinz 2007, p. 56). Hofheinz credits the launching of the widely viewed Arab media station *Al-Jazeera* in 1996 as the first symbolic step in spreading the "communications revolution" in the Middle East (Hofheinz 2011, p. 1418). Armando Salvatore, a sociologist at the Oriental Studies University in Naples (L'Orientale), sheds light on the importance of the launching of *Al-Jazeera*. He claims satellite TV enabled the public to access information not formulated under the guise of state-run media. Salvatore states that *Al-Jazeera*:

> [C]annot be overestimated: the new TV channel started to broadcast all the news which state-owned TV did not give and, most critically, to frame them via the public perception of the fading legitimacy of their governments. They did so also through such innovations like online polls and call-in programs where the audience could debate with the TV guests. Satellite TV impacted over time tremendously on the entire spectrum of old and new media, also affecting internet and the booming blogosphere from its beginning (Salvatore 2011, pp. 6–7).

The hope for change developed greatly as the internet penetrated the region in the late 1990s. Despite these hopes, it became clear a digital divide formed (Salvatore 2011, pp. 6–7). The digital divide refers to the unequal availability of technology. The divide consists of two dimensions: the access to technology and the quality of the access to technology (Allagui 2009). The digital divide in the Arab world is directly influenced by the lack of access to technology. Ilhem Allagui of the American University of Sharjah, attributes this lack of access to the restrictions governments place on the population as a result of fear that the internet could mobilize the public against them. Allagui notes governments are not entirely to blame for the lack of access to the internet. She discovered the people themselves also share the responsibility. Many in the Arab world lack the awareness or the education to access the internet. Finally, gender gaps have also played a major role in the digital divide due to cultural standards. At the onset, women in this area were not engaged—although this is changing dramatically—in the past, women feared voicing their opinions because of possible backlash (Allagui 2009).

The introduction of the internet quickly led to the digital divide we see presently, but we do see positive trends as penetration of internet usage in the region gradually increases. Prior to the Arab Spring, the most improved country in internet penetration was the United Arab Emirates (UAE) which saw an increase of internet penetration from 35.1 % in 2007 to 49.2 % in 2008 (Allagui 2009). In 2012 the UAE penetration rate was at 70.9 % or 5.8 million users, a dramatic increase since 2000 where there were 735,000 internet users. It is important to note, the UAE did not experience a toppling of the monarchy during the Arab Spring despite its large penetration rate. Bahrain on the other hand, shows the largest penetration rate in the region in 2012 at 77.0 %, yet it only totals for 1.1 % of internet users in the Middle East (Internet World Stats 2012). Bahrain did experience protests against its government during the Arab Spring given the lack of representation among the Shiite majority which is ruled by a Sunni monarch. Although Bahrain claims it has addressed the grievances of it citizens since the uprisings, it has not made significant changes, and continues to face criticism from international human rights organizations (Fahim 2012, New York Times).

In 2012, internet penetration in the Middle East surpassed the world average. According to Internet World Stats (2012), internet penetration globally was at 34.1 %. The Middle East saw a penetration rate of 40.2 % which encompasses 3.7 % of internet users in the world. Quantified data shows the world total at 2.4 billion and the Middle East at 90 million. Iran stood as the largest internet consumer accounting for over 46.7 % of users in the region. Although the penetration rate within the country was at 53.3 %, it scored lower than its Arab neighbors; however, we must recognize, Iran is the most populated country in the region and still contains market share in this area. Iran saw significant increases since the year 2000 where the number of users increased during this period from 250,000 to 42 million in 2012. In North Africa, Egypt and Tunisia also saw similar increases since the year 2000. In Tunisia, the penetration rate was 39.1 % totaling 4.1 million users in 2012. In 2000, there were 100,000 Tunisians on the internet. Egypt's penetration rate was comparable to Tunisia's. In 2012 the penetration rate was 35.6 % totaling 29.8 million whereas in

2000, the total number of users on the internet was 450,000 (Internet World Stats 2012). Internet penetration in the Middle East continues to surpass the rates of previous years showing the internet is still showing grow and new potential.

5.2.2 The Blogosphere

Influenced partly by the advent of satellite television, the Blogosphere emerged in the Middle East as the first milestone in developing the path for cyberdemocracy. Blogging in the Arab world first started in 2005 and was influenced by the rapid expansion of blogging in Iran. Egypt became the Arab leader in blogging. The first Egyptian bloggers began writing about several issues in society that spanned from abuses by state authorities to sexual harassment. These efforts did gain international attention and did see reaction from the state to enact legal action against violators, yet it was not monumental (Hofheinz 2011, p. 1419). Finding concrete data on the number of Egyptian bloggers is difficult to find, but it is clear the blogosphere in Egypt started with a handful of blogs and expanded exponentially. The average blogger in Egypt is considered educated, equally male or female, under the age of 30 and originates from the middle or upper class (Rifaat 2008, pp. 51–52). In addition, young supporters of the Muslim Brotherhood (the main Islamist opposition group in Egypt) also began utilizing blogging around this time. Their injection into the Egyptian blogosphere created a divide within the sphere between secular and Islamist bloggers (Salvatore 2011, p. 7). Hofheinz helps form a conclusion on the impact of the Egyptian blogosphere stating that blogging failed to topple the regime leading to crack downs and leaving the "fatigue [of] Egyptian Blogging" (Hofheinz 2011, p. 1419).

In Iran the blogosphere developed more vibrantly and took a stronger foothold as a model for the region. Iranian blogging first emerged through a young journalist named Hossein Derakhshan who began blogging in Toronto, Canada shortly after September 11, 2001. Derakhshan began voicing opposition to the Iranian regime by posting instructions on the Internet in Persian on how to create a blog. Derakhshan was named the "Father of Iranian Blogging." In 2006, Derakhshan successfully made Persian the tenth most used language on the internet (St-Louis 2010, p. 1). The Iranian blogosphere is diverse and is categorized into two segments: (1) blogs inside Iran and (2) blogs formed by the Iranian diaspora. Hervé St-Louis in his analysis *Iranian Political Unrest in Cyberspace* formulated a vision of what Iranian blogging "is" through the impressions of a Tehran based British journalist. Angus McDowall states that

> …while Iranian bloggers vividly portray a genuine part of Iranian society, they are a self-selecting sample that consist mostly of young, affluent, liberal-minded people who do not represent 'the real' Iran." He added, "What we rarely see in the English-language blogs are the views of a car-parts worker in the Khodro factory in Karaj, the unemployed young man who smokes heroin in a new, cheap housing estate on the edge of Semnan, or a housewife in Mashhad worrying whether her kids will get a place at the university. These people are as much 'the real Iran' as the bloggers, but their voices are less often heard (St-Louis 2010, p. 6).

The domestic base of Iranian bloggers do attempt to draw western attention to their content regarding the political situation in Iran. St-Louis cites research conducted by Harvard University's John Kelly and Bruce Etling who have mapped the domestic Iranian Blogosphere. They conclude it comprises of four subgroups. The first is the secular/reformist group which consists of journalist and dissidents who orient their content towards political affairs. The second is the conservative/religious group which splits into two subgroups. The first subgroup being aligned to the conservative Shi'a regime, attempts to promote the Shiite worldview and also criticizes the regime's leaders. The second subgroup attempts to build awareness of the Twelver branch of Shi'a Islam. They focus on preparing the world for the return of the Twelfth Imam, the al-Mahdi. The third group is the religious youth which is viewed as the "Persian poetry and literature subgroup because blogs in this category feature poetry and literature from Iran" (St-Louis 2010, p. 7). Kelly and Etling found that this group parallels the conservative/religious group suggesting this group is coordinated by the regime. The final group is the "mixed network" which is general in nature, covering personal topics and sports (St-Louis 2010, p. 7).

In 2010, there were over 700,000 bloggers in Iran. Like in Egypt, Iran was also exposed to the revolution of satellite TV. Although the state attempted to control the satellite TV, these efforts were later abandoned (Litvak 2011, p. 4). Iran was also the first nation to execute a blogger and establish the Cyber Army through the Iranian Revolutionary Guard Corps (IRGC) (Litvak 2011, p. 11). According to Australian journalist Antony Loewenstein, there are key differences between Egyptian and Iranian bloggers stating "[u]nlike the Egyptian bloggers who lost their fear of the regime, Iranian bloggers exercised self-censorship out of fear of the regime" (Litvak 2011, p. 11).

Although Hofheinz references the "fatigue of blogging" in Egypt. His research on Islamist groups working within the framework of the internet cannot be overlooked. Islamist groups have been using the internet to also proliferate their worldview. In 1993, several Islamist groups in America and Europe established widely read mailing lists to spread awareness of aggression on Muslim communities throughout the world; namely Palestine, Chechnya, Bosnia and Kashmir. As technology improved, they shifted to full websites and news aggregation. Extremists also utilized chatting venues most often through Yahoo! The outcome of the revolution in Egypt led to the empowerment of the Muslim Brotherhood, and his research offers insight showing the mobilization of online activists were not solely in the secular camp (Hofheinz 2007, p. 72).

In 2005, Islamists were keen on using technology to influence the outcomes of municipal elections in Egypt and Saudi Arabia. Islamist groups were actively using the internet and SMS (Short Message System or Text Messaging) to promote clerics in Saudi Arabia. Hofheinz points out it was no surprise "Golden List" candidates (a directory of Islamic leaning candidates under the umbrella of the social trend, Islamic Awakening), won local elections despite being banned from running as a political party. Egyptian Parliamentary elections in 2005 saw similar efforts with the Muslim Brotherhood successfully mobilizing voters. The Muslim Brotherhood was effective in using email, websites, SMS, and a strategy of house

to house campaigning to bring out the vote. It left many commentators, including secular ones, to marvel at their success. Hofheinz shows that internet traffic on the Islamist web platform Ikhwan Online shadowed the traffic that was experienced on the secular Kefaya movement's website (Hofheinz 2007, p. 73). Although the fatigue of blogging may have settled in, it is clear the advent of the blogosphere set the stage for a new avenue of outreach and revolution embodied in social media.

5.2.3 The Dawn of Social Media

Social Media was the new evolution for cyberdemocracy in the Middle East. The evolution of social media in the context of the Middle East and more specifically during the Arab Spring has been debated by experts who monitor these trends in the region. Several questions develop when looking at this subject. How effective was social media in the Arab Spring? What did social media do that blogging could not? Was social media during the Arab Spring intended for domestic consumption or was it predominantly consumed by the outside world? In order to understand these trends with greater insight, we must identify the usage in the region and further understand its development in its modern context.

Several social media tools were utilized during the Arab Spring. Two social media sites that stand out above the rest where Facebook and Twitter. According to Facebook's website, the mission of the site is to "give people the power to share and make the world more open and connected" (Facebook.com). Facebook enables a site user to publish their entire life story through a form of a digital diary. It enables one user to connect to other users who they may have an affiliation with: a close friend, family member, acquaintance, or a random person. In addition to connecting members together in one place, it also gives users the ability to form groups surrounded by a common interest or cause. Twitter on the other hand, "is a real-time information network that connects you to the latest stories, ideas, opinions and news about what you find interesting" (Twitter.com). It enables its users to post short messages that contain 140 characters or less in the form of a tag line. In addition to raw text, a user can embed hyperlinks to websites, articles, pictures, and additional content found on the web. On one screen, a member can aggregate information quickly related to a wide array of content and more specifically current events.

Usage of both sites continue to grow at a fast rate. According to Internet World Stats (2013) the number of Facebook users in the Middle East as of December 31, 2012 totals at 23.8 million achieving a 10.6 % penetration rate among internet users in the region. Unfortunately, this data is not quantified for Iran and Syria. In the United Arab Emirates the number of Facebook users stands at 3.4 million with a penetration rate of 41.7 %, while in Saudi Arabia there are 5.8 million users with a penetration rate of 22.1 % (Internet World Stats 2012). In North Africa, particularly in Egypt, the number of Facebook users totals at 12.1 million achieving a 14.5 % penetration rate. In Tunisia the number is smaller at 3.3 million users, but penetrating at 31.0 % of internet users in that nation (Internet World Stats 2012).

Twitter continues to hit milestones as more users in the region are exposed to its reach. According to the Arab Media Report, the number of Twitter users globally as of February 2012 stands at 500 million users "tweeting" over two billion "tweets" a week. As of June 2012, the number of Twitter users in the Arab world numbered at two million averaging 5.75 million tweets per day. Although Turkey continues to be the leader in the Middle East, Egypt consists of the largest Twitter users in the Arab world with 129,711 users. The top five Arab countries using Twitter are Egypt, Saudi Arabia, UAE, Lebanon, and Qatar. In terms of penetration, we see a divergence in the number of users to penetration ratio. Even Turkey with its users approaching 600,000 straggles at 2.02 % behind countries like Kuwait (12.8 %) and Bahrain (5.33 %). Egypt's penetration rate was only at 0.35 % as of June 2012 (Mourtada and Salem 2012, pp. 15–16).

Despite the attention that Twitter drew on the Arab Spring, we find the microblogging site continuing to grow at a rapid pace, but not surpassing the rate of other social media networks. The Arab Media Report sheds light on this trend when compared to LinkedIn usage. LinkedIn is another social media tool similar to Facebook, but it is predominately used as a networking tool for business professionals to link together on the premise of a business nature. The number of LinkedIn users as of June 2012 was 4.2 million with an average penetration rate of 2 % across the Arab world showing the number of LinkedIn users double the number of Twitter users (Mourtada and Salem 2012, p. 19). According to the Arab Media Report, "Twitter penetration remains behind that of LinkedIn—except in Kuwait—indicating that job hunting and professional networking services through LinkedIn are more relevant in the region than the informational, social and political uses of social media that Twitter provides" (Mourtada and Salem 2012, p. 22).

YouTube was a major source of video content documenting the events during the Arab Spring and the Iranian Green Revolution. Although the majority of the content viewed during these periods were considered gruesome, they were also eye-opening and brought forth a front row seat to the situation not covered by conventional media. To cite the Arab Media Report, YouTube promoted citizen journalism and "is arguably the primary social networking platform that effectively established the strong convergence between traditional broadcast media and social media in the Arab region" (Mourtada and Salem 2012, p. 23). YouTube usage continues to grow at a fast rate. There are over 167 million video views on the site a day in the region only trailing behind the United States. In Egypt, uploads were up 150 % and views increased by 220 % from 2010 to 2011. Comparatively, Saudi Arabia's uploads were up 200 % and views increased 260 %. In Egypt over 41 % of YouTube users are women, the average age of all users are 35 with 67 % having university degrees. Findings showed 28 % of YouTube users access the internet through a smartphone while 19 % of these users access the YouTube site via a smartphone. Saudi Arabia on the other hand proved to show differences. Primarily in the area of gender comparison, 50 % of YouTube users in Saudi Arabia are women. The average age is lower at 33 years old. Finally, 36 % of Saudi users have university degrees and over 65 % of Saudi's access the internet via smartphone (Mourtada and Salem 2012, p. 23).

5.2.4 *Restrictions on Cyberdemocracy in the Region*

Many regimes in the Middle East faced a difficult choice in introducing the internet into their societies. On the one hand, they fully understood the importance of the internet, yet on the other, they were aware of its dangers. For most states in the region, the internet was both a blessing and curse. This feeling was best described in former Egyptian President Hosni Mubarak's words:

> The effects of the revolution in ICTs [information and communication technologies] should not be limited to achieving economic and developmental gains. They should be extended to strengthening political, social, and cultural links among nations to bring about world peace based on justice, equality, and…supporting national efforts toward more freedom, democracy, and respect of human rights" (Zarwan et al. 2005, p. 20).

The rise of the Internet Café has been a predominate point of access to connect to the internet in many of these countries. These cafés provide an affordable avenue for many in the region to access the web. They have also been targets of crackdowns and filtration in many respects due to their popularity. During the Mubarak era, "free" internet programs were started to encourage any Egyptian with a computer, modem, and a phone line to access the web. The programs enabled many Egyptians to connect to the internet for less than the price of a phone call. The outcome of this promotion led to detentions, more monitoring, and entrapment. Opposition group websites were blocked and their members arrested for posting their views online (Zarwan et al. 2005, pp. 3–4).

Egypt in many respects was viewed as a model for the developing world in expanding internet access. The government went as far as starting the "PC for Everyhome" initiative where Egyptian families could afford to purchase a computer through a credit system. The "IT Clubs" and "Smart Schools" initiatives provided rural areas and schools the ability to access the web where before it was not possible. Finally, Egypt even promoted "e-government," enabling Egyptians with the ability to streamline access to government records and information (Zarwan et al. 2005, pp. 19–21).

Despite these efforts, the Egyptian government moved to filter and monitor the internet. Egypt began policing the internet in September 2002 when the Interior Ministry launched the General Administration for Information and Documentation (GAID). The primary function of this group was to monitor the internet in real time to protect the integrity of morality in society and prevent cybercrime. In the early days of monitoring, online pornography was a major target for censorship. Restrictions were slowly lifted as complaints from competitor internet service providers (ISPs) who were losing business to ISPs who were not filtering pornographic material. It appeared the discussion of internet pornography evolved into a matter of personal responsibility and self-censorship, rather than public concern. The Egyptian government was concerned with the recruitment of militants willing to engage in violence under the influence of the internet. This fear was often the justification for human rights abuses against activists. Human Rights Watch cites several case studies of individuals who faced repression from the government due to online monitoring (Zarwan et al. 2005, pp. 25–28).

The Gulf States also use similar restrictions on the internet. Saudi Arabia allowed internet access in 1999, and later in 2001 launched its internet police, the Internet Services Unit (ISU). The ISU continues to block web access to websites and blogs, and is often boasting about its efforts in this area. In Bahrain, websites are required to register with the Ministry of Information where they have blocked several websites and have also arrested web moderates over content viewed as critical of the ruling family. The UAE through the sole ISP, Etisalat also blocks several websites that contain pornographic material, gambling, gay and lesbian content, and minority faith websites. Furthermore, ISPs are required by law to report user information to the Ministry of Post and Telegraph as is in Bahrain (Zarwan et al. 2005, pp. 4–5). In November of 2012, the UAE placed tougher restrictions on online dissents, making it a crime to mock its rulers or organize unauthorized demonstrations. Although the UAE did not experience mass demonstrations as seen during the Arab Spring, the passage of this legislation increases restrictions on free speech. Furthermore, several arrests were made and in certain cases deportation of dissidents was witnessed (BBC News 2012).

Iran in comparison to the Gulf States and Egypt falls in line with the general trend of the region's restrictions on the internet. Like Egypt, Iran also invested heavily in developing online access and growing internet users. Several key members of the government including Iran's Supreme Leader, Ayatollah Ali Khamenei, participate online by developing their own blogs, a common tool many Iranians use online. Iran is conscious of controlling the media by cracking down or closing print and television media all together (Zarwan et al. 2005, p. 20). Web media is a primary source for voicing opposition against the government today. The Iranian government has retaliated against journalists, bloggers, and technical staff through imprisonment and blocking their content online. Interestingly, the Iranian constitution states, "the investigation of individuals' beliefs is forbidden, and no one may be molested or taken to task simply for holding a certain belief" (Zarwan et al. 2005, p. 44). Other examples of prohibition of censorship in Iranian law are present and suggest censorship is not tolerated, yet violations of these statues continue.

To conclude on identifying the tools of cyberdemocracy in the Middle East, we are still on the horizon of a new frontier. Disseminating what is truly going on is a major focus. Since the inception of the worldwide web, the Middle East and more specifically the Arab world are growing with global trends. As the use of social media grows in the west, it is also true for the Middle East. The quantified data uncovered in this section shows there is more potential ahead. Penetration rates of online usage in a majority of these countries is still not at the levels sustaining the argument that the internet birthed the revolutions of the Arab Spring alone, yet we cannot underestimate its role nor its potential for the future. Social media is used most heavily by users in parts of the region where change did not take place. This was particularly seen where social media sites like Facebook and Twitter are more widely used in Gulf States like Saudi Arabia and the UAE. No toppling of those regimes materialized, but these states enacted tougher policies to curb online activism since the Arab Spring. Shifting to the traditional reasons for revolution, we aim to uncover the underlying issues in Egypt and Tunisia that further enhanced the need to call for change. It leads to this question, what was the tipping point? The next section will present an analysis of a case study for Egypt.

5.3 Egypt: Case Study for Cyberdemocracy and Underlying Realities of the Arab Spring

The revolution in Egypt showed that mobilization and mass protest encouraged change, yet we cannot underestimate the underlying realities encouraging activists to take to the streets and protest. The basis for these revolutions were based predominantly on the "politics of bread." Economic strife was the cornerstone of the will to protest. The general consensus is the Arab Spring began after the vegetable vendor, Mohamed Bouazizi, immolated himself in Tunisia on December 17, 2010. Bouazizi's act sheds light on the underlying realities and frustrations shared by a majority of people in the region. In a desperate call for help, Bouazizi sparked a call for change. So who was Mohamed Bouazizi? Hernando de Soto of the Institute for Liberty and Democracy describes him in this light:

> As is so often the case with political martyrs, Bouazizi means strikingly different things to different people. To some he's a generic symbol of the resistance to injustice; to others an archetype of the fight against autocracy… It is hard to imagine that the real Mohamed Bouazizi would have recognized himself in any of these incarnations (De Soto 2011).

Bouazizi was a simple man trying to provide for a better life for his family. He was a struggling entrepreneur who at young age was responsible for sustaining his entire immediate and extended family. De Soto qualifies him as a repressed entrepreneur who faced "insurmountable obstacles" in his way. He regularly faced corrupt local officials who stole his products, arbitrarily fined his business, and sought bribes. His fate would change on the morning of December 17, 2010 when he was confronted by two inspectors for not paying a fine. His products were seized along with an electronic scale he used to conduct business. He was publicly embarrassed after being slapped by a female police officer, and after failing to appeal his case, he set himself on fire in front of the government building in his home town of Sidi Bouzid.

This story was far too familiar for many in the Middle East, many dealt with the same disenfranchisement. Bouazizi was "deprived of the only thing that stood between him and starvation—the loss of his place in the only economy available to poor Arabs" (De Soto 2011). There were an additional 35 acts of self-immolation in the Middle East and North Africa following this incident. The Bouazizi story and tragedy is a common one in the Middle East. A down-trotted entrepreneur set on making a better life for his family while facing repression by the state. As the story relates to the Arab Spring, understanding the how of this event, is equally as important as understanding the why of this event. Political and socioeconomic inequalities played a major role leading up to the Arab Spring. We shift from Tunisia to Egypt to identify a case study where these factors played a role.

5.3.1 Egypt Prior to the Revolution

The Egyptian economy was performing at peak levels prior to the revolution. Noha Bakr explains that GDP growth had increase to 7 % in 2007 and 2008 as opposed to being below 5 % levels in the mid-1990s. Foreign investment from 2004 to 2009

was at $46 billion, exports tripled, and foreign debt was shrinking (Bakr 2012, p. 58). In addition, major sectors of health, education, access to technology were improving. Unfortunately growth in Egypt was not seen in all areas of Egyptian society. Unemployment was at 9.7 % while heavily concentrated among young people with degrees (Bakr 2012, p. 64). The socioeconomic situation in Egypt also created motivations for change. The population grew rapidly from 57.8 million to 83.1 million from 1990 to 2009. Over 23.5 % of the population was between the ages of 15–29, characterizing Egypt as a young country (Bakr 2012, p. 59). The infant mortality rate increased along with decreased rates in malnutrition, and the average life expectancy rose from 64 years to 71. In addition, the extreme poverty rate was at 6.1 % in 2008 and 2009. The poverty rate has increased in the aftermath of the revolution, yet in 2008–2009 the poverty rate was 21.6 % and rose to 25.2 in 2010 and 2011 (World Bank 2013). Illiteracy rates dropped; however, the quality of education did not prepare young Egyptians to compete in the labor market. The ethnic and religious disparities also presented challenges. Egypt is divided predominantly into two religious groups: 90 % Sunni Muslims and 9 % Coptic Christians. Ethnic groups in the country consist of Nubians, Sinai Bedouins, and Bedouin tribes along the western border with Libya. Bakr notes religious, and ethnic lines, stating all segments had "grievances and refrain from sharing in the fruits of development" (Bakr 2012, p. 59).

Technological development was soaring, the IT revolution in Egypt granted more access to the public than ever before. The Egyptian government made heavy investments in improving technology and access to the internet. In June 2009 over 3,211 IT companies existed in the country. Expansion was dramatic, leading to the media sphere comprising of "21 daily newspapers and 523 other forms of publications, as well as 700 Arab speaking TV channels, the majority of which broadcast ferocious political talk shows" (Bakr 2012, p. 60). Like Noha Bakr, we ask the following question: if the economic and social situation in Egypt was improving, then why did the revolution happen?

The political landscape in Egypt did not compare to the economic improvement seen prior to the revolution. As Bakr puts it, Egyptians were becoming cynical and bitter with the political process and the 30 year reign of Hosni Mubarak. Moreover, Bakr notes the alienation among the youth as manifested on Facebook through slogans stating: "Egypt isn't my mother, Egypt is my step mother" (Bakr 2012, p. 61). Constitutional reforms in 2005 also contributed to further discontent with the Mubarak regime. Reforms were concentrated on evoking hereditary rule followed by fraud in parliamentary elections (Bakr 2012, p. 61). Mubarak attempted to transfer power to his son Gemal Mubarak (Steiman 2012, p. 5). People also viewed Egypt's regional and international policies as weak. In many dimensions, Egypt's hegemony on Arab culture diminished from prominence unlike the 1960s and 1970s (Bakr 2012, pp. 61–62). Human rights abuse cases were no longer going unnoticed by Egyptians. Intolerance of minorities, particularly in the case of Egyptian Copts, enabled outrage as the government did not react to protect these minorities (Bakr 2012, pp. 65–66).

5.3.2 The Revolution

Despite previous failures to mobilize protestors through social media, a young man's brutal death would spark enough outrage to influence the masses to take to the streets. Khaled Said on June 6, 2010 was heading toward an internet café and was intercepted by police officers who beat him brutally to death in broad day light (Trew 2013). Inspired by Said's tragedy and the quest to seek justice for his death, Wael Ghonim launched a Facebook page titled "We are all Khaled Said." Unaware of the impact his Facebook page would bring, he began to mobilize people online. Encouraged by the self-immolation of Mohamed Bouazizi in Tunisia, Ghonim called for a revolution through his Facebook page on January 25, 2011. Protestors flooded into Tahrir Square crying for "bread, freedom and human dignity." Their demands were broadcasted around the world through television and the internet. Ghonim was arrested on January 27 and beaten and tortured for his role in collaborating protests, his emotional interview to the press further encouraged protestors to take part in the revolution (El-Arian 2013). During the revolution, over 34 million people participated on Facebook on 2,313 pages. Inside and outside of Egypt, over 93 million tweets referencing the revolution were tweeted on Twitter. The price for the revolution cost the lives of 846 Egyptians and left 6,467 wounded (Bakr 2012, p. 68).

The Mubarak regime held its position in the face of protest, but the tide changed and the regime fell short of managing the crisis to maintain control. The regime responded with more brutality against protestors through intimidation, and cutting access to the internet and communication. Mubarak offered halfhearted gestures of reform. He dissolved the parliament and agreed not to participate in presidential elections in September. His efforts fell on deaf ears. Protestors called for his resignation and would not accept any other action. Mubarak addressed the nation on February 10th and proclaimed he would delegate his authority, yet still remaining in power. As a result, the crowd was not pleased and continued to call for his resignation. On February 11th, the 30 year reign of Hosni Mubarak came to an end (Bakr 2012, p. 66).

5.3.3 The "Inaction" of the Military

The reaction from the military during the revolution was surprisingly neutral. The military faced a difficult choice as it related to their place in the revolution. On the one hand, they could have supported the Mubarak regime and maintained their power; yet on the other, if the revolution succeeded, they would face unprecedented dissatisfaction. The military was viewed as a professional, powerful, and highly respected institution by the Egyptian people. Prior to the revolution the military benefited greatly from the Mubarak regime. Their cooperation with the regime enabled the military establishment to enjoy lucrative business opportunities, yet

within the last 10 years, the military began to lose respect for Mubarak. The attempt to bolster his son as a successor to the presidency was not favorable among the military ranks. Furthermore, Mubarak's efforts to create a system of crony capitalism without the military was also looked down upon. Mubarak ignored the military's influence in the political realm when it came to appointees and policy (Steiman 2012, p. 5). The presidency in Egypt was always reserved for high ranking military commanders including Abdel Gamal Nasser, Anwar Sadat, and even Hosni Mubarak. Finally, the military had to protect its image in the eyes of the Egyptian people. They had succeeded in portraying this image until they took control through the Supreme Council of the Armed Forces in October 2011. The military later showed its might through various crackdowns, particularly against Copts in a bloody quelling of a protest—this lead to shock and anger. Daniel Steiman concludes the military's actions were guided by two motives: survival/maintaining power and material gain (Steiman 2012, p. 7). The military's efforts were very critical in determining the outcome of the revolution. If the military had interjected like their counterparts in Iran, Mubarak may have maintained power. Their decision to not intervene aided in making Mubarak and the Egyptian people understand the end was in sight. Mubarak alienated the military from taking advantage in the fruits of economic prosperity and political influence. In the end, the military made a tactile decision and survived.

5.3.4 Consequences of the Revolution

For Egypt, change yielded consequences. The economic and political situation in Egypt was greatly affected. On the political front, the Supreme Council of the Armed Forces (SCAF) took power after Mubarak's resignation. SCAF was viewed as the defender of the revolution, but eventually began to lose credibility as it moved to remodel Egypt to mirror the constitutional system of Turkey. The military in Turkey maintained a strong role in politics and could interject in the political sphere if it felt the nation was straying from the original framework of the republic model founded by Mustafa Kemal Ataturk. The Egyptian public did not view this as a favorable outcome for the new Egyptian state and began to disapprove of it (Bakr 2012, p. 73).

Several election cycles took place from November 2011 to January 2012. The Muslim Brotherhood's Freedom and Justice Party gained 46.3 % of the vote, but combined with the Salafist Nour party the Islamists camp accounted for 70 % of the seats in parliament. Liberal groups were hugely underrepresented as result of their lack of organization and internal rivalries. In June 2012, the Supreme Court dissolved the lower house of parliament a few days before the presidential run-off election. The Islamist succeeded in electing the Muslim Brotherhood candidate Mohamed Morsi as president (Körner et al. 2013, pp. 2–3). The military attempted to maintain power after Morsi's election, yet Morsi responded by retiring top level military officials. Thereafter, a constitutional assembly was set in motion to create

Egypt's new constitution. In November 2012, a decree by Morsi exempted presidential decisions from judicial review and prevented the court from dissolving the body responsible for drafting a new constitution. Finally in December 2012, the drafting of the new constitution was completed and approved in a popular referendum. The constitution was met with criticism as the opposition voiced concerns for the legislation on the subject of the rights of women and minorities (Körner et al. 2013, p. 5).

The economic fallout of the Arab Spring in Egypt was equally concerning. Following the revolution, the real GDP decreased dramatically to −4.2 %. Investment dropped by 26 % and net exports decreased by 3.6 % since the third quarter of 2010 (Bakr 2012, p. 71). The production process was crippled by mass demonstrations and strikes. Tourism levels were at some of the lowest levels seen dropping by 40 %. Foreign direct investment in the region was impacted by the revolutions in Tunisia and Egypt dropping by 46 %, the same levels as in 2004. In 2012 net exports significantly dropped by 5 % in Egypt and Tunisia. Foreign currency reserves also dropped as a result of the Arab Spring. Finally, the fiscal debt accounted for 11 % of the Egyptian GDP in Fiscal Year 2011/2012 (Körner et al. 2013, pp. 6–8).

The revolution had its heartaches. The political, economic, and social situation in the country further divulged into a state of affairs not envisioned by all groups who participated in overthrowing the Mubarak regime. As a direct consequence, the situation in Egypt is at an unclear roadblock. Although it is true, a government stands in place today, determining the longevity of this new government is still in question. It is of no surprise the Islamist camp claimed power. They were the most organized, and also utilized the same cyber tools employed by their secular counterparts. The fact remains, the Islamists were more united, better organized, and had more experience in Egyptian politics. They worked around the repression delivered by the Mubarak regime, the military, and the secular movement and still succeeded. However, the success of the Muslim Brotherhood was tested after the military staged a coup on July 3, 2013 after 1 year of Morsi's presidency. Morsi was placed under house arrest and was ousted from the presidency. The military designed a roadmap that attempted to steer the country in the direction the revolution had originally intended.

We shift now our discussion to Iran and analyze what went wrong in Iran as opposed to what went right in Egypt.

5.4 Failures in Iran

The Iranian presidential election of 2009 set the stage for the Arab Spring to flourish. Unlike its Arab neighbors, Iran did not see the ousting of its government. Named after the color of the opposition movement to the incumbent president, the "Green Revolution" or the "Green Movement" refers to the massive protests following the 2009 elections. In this section, we aim to understand why the Green Revolution did not succeed in overthrowing, or much less reforming the Islamic

Republic. Iran's history in the political context has endured several changes. The overlapping theme in Iran's political development is heavily influenced by the nation's effort to thwart foreign influence from its domestic affairs. Although having been subjugated to the will of foreign influence, Iran in the later part of twentieth century developed a system, where in its view, eliminated these influences and created a system that is uniquely its own. The state's view of itself is still at the center of debate among its domestic population and its diaspora aboard. A brief history of Iran's political development during the twentieth century will create a point of reference leading to the events surrounding the Green Revolution.

5.4.1 Iran: A Brief Political History of the Twentieth Century

Revolutionary trends are nothing new for Iran. The country endured several revolutions during the twentieth century. The Constitutional Revolution of 1906 established an elected parliament (the Majlis) and a constitution limiting the power of the Qajar monarchy. The revolution successfully established these changes as a result of different factions fighting to limit the power of a corrupt government. Later in 1925, the Pahlavi Dynasty was established through the efforts of a military coup removing the Qajar Dynasty under the direction of the Persian Cossack Brigade. The commander of the Cossack Brigade, Reza Pahlavi, succeeded the throne of the Qajars and established his dynasty as the new Shah of Iran. Reza Pahlavi was succeeded by his son Mohammad Reza Pahlavi, the last Shah of Iran. In 1953, a coup orchestrated by The United Kingdom and The United States overthrew Prime Minister Mohammad Mosaddeq. Western powers were concerned Mosaddeq was sympathetic to communist influence. These fears were heighted by Mosaddeq nationalizing Iran's oil industry. The Shah briefly fled the country only to return after military forces quelled riots and restored the Shah's authority. Mohammad Reza Pahlavi's reign in Iran ended with the "Islamic Revolution of 1979." The Shah's efforts to repress opposition through his secret police, the SAVAK, and his deteriorating image among Shi'as lead to great dissatisfaction in Iran. The revolution, headed by Ayatollah Khomeini, who through the use of audio cassettes, was able to spread his message of revolution to the people of Iran. Since the Islamic Revolution, Iran transformed from a monarchy to an Islamic Republic, and has remained an Islamic Republic since.

5.4.2 The 2009 Election and the Green Revolution

After presiding over his first term as the President of the Islamic Republic of Iran, Mahmoud Ahmadinejad was up for re-election in June 2009. With record breaking turnout, Iranians on June 12th went to the polls with the ambition of electing a new president of the Islamic Republic. After a very energetic election campaigned filled

with debate and vigor for the candidates, Iranians went to the polls. Shortly after the polls closed, the Interior Ministry determined incumbent President Mahmoud Ahmadinejad was re-elected president by a 62 % majority. In the final days of the election campaign, rallies in support of the main opposition and reformist candidate, Mir Hossein Moussavi, showed fleeting support for Ahmadinejad. Although Ahmadinejad gained support in the rural segments of the country, unemployment and growing inflation were a leading factor in the reduction of Ahmadinejad's popularity. Ahmadinejad was essentially viewed as a populist candidate who helped increase benefits to the people. The growing support for Moussavi became alarming to the military establishment and lead the commander of the Iranian Revolutionary Guard Corps (IRGC) to decree that any revolutionary activity in light of the election results would be dealt with harshly. As the ballots were being counted, the Iranian government reportedly shut down Internet sites and mobile telephones while deploying security forces and the youth volunteer corps Basij in the streets of Tehran. Once voting was concluded, both the Ahmadinejad and Moussavi campaigns declared victory. Allegations of voter fraud were announced and the government moved to investigate the matter, but required this be conducted through legal channels. After massive disappointment of the government validating the election in favor of Ahmadinejad, Iranians took to the streets in protest. Widespread protests throughout the country directed the government to send in the IRGC and Basij forces to quell the uprising with tear gas and weapons.

5.4.3 The Green Revolution in Contrast to the Arab Spring

The Green Revolution and the Arab Spring where different on a number of levels. Like its Arab neighbors, Iran is a young nation. Over 60 % of the population is under the age of 30, and reformist efforts have been actively utilized since the inception of blogging and social media. Unemployment among the youth is also a major issue. According to the CIA, both unemployment and inflation rates were both at 20 % while unemployment for the youth was estimated at 23 % (Litvak 2011, pp. 3–4). Protests against the outcome of the 2009 presidential election was primarily based on the disenfranchisement of the vote. Voters in Iran genuinely believed that their voice was going to be heard. The government turned its back on the very principles it claims to uphold. This yielded a loss of "faith in the system as a whole" (Litvak 2011, p. 8).

Like in Egypt, the economic system in Iran was equally filled with economic nepotism. The IRGC was a major benefactor of this arrangement claiming major stakes in the "oil [industry], construction, agriculture, mining, transportation, defense industry, and import/export" (Litvak 2011, p. 8). Loyalty to the regime was further enhanced on the economic front. Shortly after the Islamic Revolution of 1979, the government linked the wellbeing of the people to the state through Bunyads, employing hundreds of thousands through this system of economic patronage (Litvak 2011, p. 8). As in Egypt, literacy rates in Iran increased significantly

since the Islamic Revolution. Iran's "thirst" for the written word reached new heights, and is still actively counteracted by the government (Litvak 2011, p. 3). Litvak describes Iran's internet usage in this way: "[I]t is safe to say that 32 years of Islamic rule have led to the erosion of Islamic ideology among segments of Iran's younger population. Culturally, Iranian youth are increasingly shunning traditional norms and constantly testing the country's restrictive laws" (Litvak 2011, p. 4).

Support for Moussavi and the Green Revolution eventually came undone. The Green Revolution was quelled by the security apparatus in Iran and as a result, the collateral damage of this event could not be over looked. Incorporating Meir Litvak's commentary on the aftermath of the revolution, he finds that there is still a case to be made for democratization in Iran, but he conveys the contrast to the Arab Spring. One of the many challenges facing Iranians living within the context of the Islamic Republic relates to the vision the Islamic Republic has of itself. As alluded to in the beginning of this section, the Iran-West dichotomy ("East–west" dichotomy) on reforming the regime is in constant contention with the liberal segment of society and the religious establishment. Litvak's interpretation on this matter is appropriate:

> Consequently, the debate has two contradictory characteristics: the first is the presentation of a sharp, almost essentialist, dichotomy between East and West in an effort to demonstrate the superiority of the Islamic concept over the Western ones, such as the universal declaration of human rights. The second is the effort to show similarity between various Shii concepts and the ideas of leading Western thinkers such as Jean-Jacques Rousseau and Emmanuel Kant, in order to demonstrate to Iranians that they need not look outside their country for inspiration. Consequently, all current Iranian leaders pay lip-service to the ideas of freedom in order to demonstrate that the Revolution and regime do not oppose it, but merely give it a different interpretation, which is highly superior to the Western view (Litvak 2011, p. 6).

This is the most difficult obstacle to overcome if we are to see real reform in Iran. Eliminating foreign influence from Iran's domestic affairs is a major theme that has shaped Iran's political development. Even if the reformists were to seize control of the regime, how could they make the case to reform the Islamic Republic into a western style democracy? The Islamic Republic of Iran is a uniquely Iranian concept. A conflict of ideology presents itself as an obstacle for reform, even with a young population in Iran, overcoming this issue has proved difficult.

Litvak presents three reasons for the Islamic Republic's longevity following the Green Revolution. One, Ahmadinejad's populist agenda enjoyed a considerable amount of support domestically. His efforts in campaigning and providing economic subsidies to the provinces was well received and gained loyalty from his followers. The second advantage focuses on linking international prestige with Iran's nuclear program. As noted by Litvak and Bakr, the Arab States lost their prestige on the international front. In the eyes of a majority of Egyptians, Mubarak was seen as a western puppet. Whereas in Iran, its national image and pride were enhanced by the state's resistance to the international community's pressure to increase transparency on its nuclear program. Finally, general disillusionment among the population leading to the sentiment of "escapism" enables the regime to encourage it as a means of detracting political dissent (Litvak 2011, pp. 12–13).

At the time of the Green Revolution, the Iranian regime was successful in making preparations to counter revolutionary trends by controlling communication and online activity. The military and security apparatus reacted immediately and brutally in preventing the protestors from taking over. In Egypt, the military remained neutral during the revolution. Only after Mubarak left the country did the military take action. Secondly, the leaders in the Green Revolution were not prepared or organized to take control of the protestors. The argument for revolution was not reinforced, their focus was "voter fraud," not overthrowing the regime. In addition, many of the leaders in the Green Revolution were either active members of the regime or were formerly regime officials (Litvak 2011, p. 11). Finally, foreign intervention in both the Arab Spring and the Green Revolution were also handled differently.

The international response to the Arab Spring and the Green Revolution played a major role in their outcomes. On the international level, the response was observed with caution. Neither the United States or Europe were willing to deal with the events unfolding in Iran head on. The reaction of the Obama administration may have been driven by its concern of portraying an image of interference with Iranian affairs as in the past, but this action of non-interference or expressing solidarity with the protestors did draw criticism from domestic and international audiences. At the onset of the Arab Spring however, the United States was far more vocal and willing to support the opposition in many Arab states. In Egypt, the Obama Administration applied pressure directly on Mubarak to concede power and make changes inside his country. In Libya, the Obama Administration created a coalition and provided direct military support to rebels against the Gadhafi regime. The contrast on the international level for both is starkly different. Had the West intervened during the Green Revolution, the outcome may have been different. Instead, the Islamic Republic overcame the Green Revolution and in June 2013 witnessed a transfer of power from Ahmadinejad to the new president, Hassan Rouhani, in accordance with the Iranian constitution.

The lessons learned in Iran had an impact on the Arab Spring. Iran's security apparatus was far more prepared to deal with an upheaval than in the Arab states. The Iranians had the experience in countering the threat from the Internet and were further mobilized to disorient the flow of information within the country. The leadership of the Green Revolution was not only disorganized, but it also lacked the proper message to drive people to overthrow the regime. On the economic front, at least from a statistical standpoint, the situation looked similar to its peers in the region, yet Iran's economic situation was not as bad as in the Arab states. The Arab protestor took an "all or nothing" approach to change the system. The leadership of the Green Revolution in Iran had no quarrel with the system itself, they were seeking a resolution to a disputed election rendering them uninterested in revolutionary change. Consequently, the Green Revolution worked inside the parameters of the Islamic Republic, they were not opposed to the system—they simply wanted to reform it. For the Arab states, the support for the Mubarak, Ben Ali, and Gadhafi regimes were completely diminished—there was no going back. In both cases the most organized elements won. In Egypt it was the Muslim Brotherhood and not the

Liberal factions that seized power. In Iran, the state was at maximum readiness to tackle the protestors head on. The military in Egypt remained neutral until Mubarak resigned. Internationally, foreign powers provided support to the opposition movements in the Arab states either through direct intervention or moral support. In Iran, the reaction was caution and nonintervention. For the Arab Spring, Iran served as a good example on how to use technology to its advantage. Whether through blogging or social media, technology proved to be an effective tool in calling for change.

5.5 Conclusion

"We're not like the American administration. We're not social media administration or government. We are the government that deals with reality" (Charlie Rose Interview with Bashar Al-Assad, September 10, 2013). Although Syrian President Bashar Al-Assad expressed his criticism of social media usage in American politics, his views tie into the greater impact social media had on the Arab Spring. Cyberdemocracy has played a significant role in the developments that have led to change in the Middle East, but this criticism sheds light on the value of understanding the situation on the ground. Mark Lynch, one of the founding fathers of blogging on the Middle East, expands on the negative effects of social media on the progression of the Arab Spring.

Before reviewing these "negative effects" in greater detail, we want to develop some (more general) ideas on cyberdemocracy and democratic development (see Sect. 5.5.1 below). These ideas we present as propositions for further discussion.

5.5.1 Some Principal Ideas on Cyberdemocracy, 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 2012; Campbell and Carayannis 2013). 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 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.

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 non-religious 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 may evolve. The global spreading of knowledge (also via the internet) should impose some additional effects.

5.5.2 Negative Impacts of Cyberdemocracy Post-Arab Spring

Mark Lynch outlines several hazards social media created for the Arab Spring. The first hazard was the exaggeration of the situation on the ground. Lynch was in Egypt during the protests and notes that the "apocalyptic" image presented in social media was not accurate. He concludes that social media welcomes and enjoys a crisis. Secondly, he found social media was successful in mobilizing protests rather than organizing civil society or political parties. As a result, movements found on social media were not ready to take on the challenges of finding leaders, cohesive strategies, or even interest in the democratic process. Lynch predicted that Tahrir Square would continue to be the forum of outrage and protest in a post-Mubarak world. His astute analysis was proven right in the summer of 2013 when the military regained control of the government as a result of continued protests in Tahrir Square, offering the military their own justification to take control. Consequently, the internet is responsible for the "dangerous polarization" present in the Arab world. This forced

opposing groups to retreat to their respective positions and engage in a war of rhetoric rather than creating a forum for dialogue.

In light of the internet creating the unification of the Arab political narrative of popular revolt, Lynch finds that this effort has been reversed. This reversal forced the short-lived unified political narrative to retract and focus on domestic affairs rather than creating a regional concentration for widespread democratic reform. In addition to creating regional disunity, the negatives of "sectarianism, fear, and hatred spread as rapidly on social media as do more positive ideas" (Lynch 2013). Although victory was at hand in the eyes of many, the sad realities of bloodshed in Syria was in full display on social media, leaving a hurdle for popular mobilization. Lynch also points out that social media helped create active restrictions online by other countries. Bahrain, Saudi Arabia, Oman, and Kuwait all moved to counteract the effects of social media on their people. This left many to abandon hopes of utilizing online forums to express their discontent toward their regimes because of harassment and policing of these online venues.

Syria remains at the focal point of a potential pitfall for the Arab Spring. Lynch focuses on Syria as being an area where the online experience of the Arab Spring has changed. Syria's engagement on the social media scene was relatively conducted anonymously in contrast to Egypt. The Egyptian experience proved to encompass well known individuals or groups that were present on social media. Syria was conducted more secretively because of fear. As a result, Lynch concludes Syria's engagement in the social media sphere has proved divisive. Violent images of the slaughter skewed the perception of the events on the ground leaving traditional media outlets to rely on this presentation as fact. For Lynch, the credibility of the situation comes into question. To conclude on Lynch's analysis, overall he finds that the revolutions conducted through the internet offer a mixed set of successes and failures. Lynch does not credit social media and the internet as the sole reason for the creation of Arab Spring nor are they the sole reason for the ongoing struggles. On the one hand, the internet shattered the "monopoly" on the flow of information by regimes, yet there are still many negative consequences to choose from.

5.5.3 Geopolitical Realities Post-Arab Spring

Lynch's conclusions on the Arab Spring fit the analytical conclusion found through the course of this discussion. Claiming social media was responsible for launching the Arab Spring does not produce sufficient evidence to prove that it was the sole cause for the revolutions witnessed. They played an important role, but to declare it as the sole catalyst, undermines the underlying realities that motivated people to call for change. As identified, the economic situation (and political stagnation) in Egypt and Tunisia set the stage for the motivation to hit the streets. Given that social media brought attention to these issues on the world stage through televised media and projections of these images to a western audience, we must acknowledge that the tools of cyberdemocracy took several years to develop a significant impact.

Foreign involvement in these revolutions further propelled the effective change that toppled regimes. This comparison was most apparent in the contrasting results of the Egyptian Revolution and the failed attempt of the Green Revolution in Iran. In Egypt, the United States exerted its power to change the course of the Egypt's fate. Egypt's dependence on American aid determined a need to stabilize the situation on the ground in order to maintain confidence for future relations. Iran on the other hand, had no strategic interest in cooperating with American foreign policy interests. In addition, the leaders of the Green Revolution were not attempting to overthrow the theocratic regime, they were already part of the status quo attempting to overturn the results of a presidential election.

Syria further embodies where foreign intervention in these revolutions has proven that without international pressure, materializing change is difficult. As Syria continues its civil war, the West complying with Russia's proposal to facilitate the transfer of Syria's chemical weapons to international oversight, prolongs the longevity of the Assad regime. Although social media has called for change and action to be taken against the Syrian regime for using chemical weapons against its own people, it fell short of empowering western powers to bring the Assad regime to relinquish power. As a result, the west will have to continue on focusing on online sources and media to drive its policy on how to deal with the Syrian civil war.

Egypt continues to be at the forefront of a new chapter in the evolution of its revolution. After the military coup (in 2013), restrictions on freedoms have been established to maintain control and security on the ground. The Muslim Brotherhood suffered a major blow in light of the coup and is on the offensive to regain control. The Egyptian court moved to ban all activities of the Muslim Brother in September 2013 (RT News 2013). As result of the military takeover, opposition by the Brotherhood to the military drew significant backlash and violence. What lies in question for Egypt is how the democratic process will develop under the guidance of the military. With the onset of the Muslim Brotherhood ban, a significant part of Egypt's political landscape cannot participate in the political process. This does present a unique opportunity for the more liberal elements of the landscape to become organized and yield a fair result in Egyptian politics.

Events in Turkey have shown interesting developments. Opposition to a construction project in Taksim Square and Gezi Park sparked widespread protest in the country. The debate over the project uncovered the population's dissatisfaction with its current government lead by Islamist Prime Minister Recep Tayyip Erdogan. Turkey's political system is heralded as the only thriving Muslim democracy in the Middle East founded by the reformist principles of the republic's founding father Mustafa Kemal Ataturk. The debate over the ruling party's reforms was projected to the forefront of these protests. The argument transformed from the construction project to a referendum on Erdogan's attempt to return Turkey to its traditional roots. The issue was resolved through dialogue and resorted to cancelling the project. Social media in this case yielded mobilizing protestors to produce a successful outcome for change, and further put the ruling party on notice for possible future dissatisfaction from the general populace. Attempts of Turkey, trying to join the European Union in the future, also have ramifications for political processes in Turkey's democracy.

Developments in the Tunisian political system have also brought positive changes as a result of the Arab Spring. In September 2013 the ruling Islamist Ennahda party decided to resign from power due to failures to improve the economy. Unlike Egypt, Tunisia's political development after the Arab Spring has been relatively peaceful despite two key assasinations of prominent opposition politicians. The Ennahda concluded that there needed to be more participation of opposition groups in government in order to create fair representation and cooperation. Outrage from the population over the Ennahda's link to Al-Qaeda also diminished its legitimacy (Gall 2013). The Islamists' new position was a significant change proving their program lacked clear understanding of how to run a country. Islamists throughout the Middle East ran on the "Islam is the answer" platform, yet they still must develop or show a coherent plan on how to solve the problems of the state. Many have argued that if an Islamist party were to take control, their ineffectiveness in running the state would prove to diminish their power and would foster better competition among other parties. Eventually the Islamists' political capital could diminish on this basis.

5.5.4 Cyberdemocracy Post-Arab Spring

To conclude on the cyberdemocracy in the Middle East, there are still many obstacles ahead. We realize that the advent of internet was not the sole reason for the evolution of the Arab Spring. The development of cyberdemocracy in the Middle East has been on a steady path towards expansion since the turn of the twenty-first century and continues to offer new possibilities. To rule out the impact of the internet and social media as a facilitator of change in region is also incorrect. In addition, traditional forms of media also played a key role. Televised reporting through outlets like Aljazeera was in fact the first milestone in presenting the issues through the lens of non-governmental bias, although the portrayal of the issues is still not free of its own bias. The internet and social media brought the Arab Spring to the forefront by connecting the story on the ground to an audience. As the audience became intrigued and gained a need for self-expression, the revolutions grew in reaction to the preexisting grievances and frustrations that had been brewing for some time.

As for the future of cyberdemocracy in the Middle East, the possibilities are continuing to redefine themselves, and at this point, the key players who can develop change will rely on this avenue to attempt to draw attention to their viewpoints and programs. The tools of cyberdemocracy can also influence foreign audiences to rally support to pressure their governments to take action against authoritarian states in the region. Authoritarian states will attempt to counteract these tools by placing restrictions or taking harsher actions in order to limit the potential impact witnessed by their neighboring predecessors. This will be, and has been, the case in the Gulf States and Iran. Foreign intervention whether peaceful or forceful, must be observed with caution as such internal conflicts can engulf a foreign power mutually.

The Arab Spring is still in its infancy, the countries who saw direct change in their governments will be vigilant in ensuring that their initial intensions for freedom and representative government are preserved. Changing the destiny of a country has never been easy. Revolutions, civil wars, outside forces attempting to capitalize on internal divisions have all been aids in detracting states from achieving success. America's first President, George Washington eloquently stated: "Against the insidious wiles of foreign influence (I conjure you to believe me, fellow-citizens) the jealousy of a free people ought to be constantly awake." Indeed the people of these countries will have to remain awake to such influences whether foreign or domestic. What can be said is that Cyberdemocracy has opened a new avenue for demonstration and uniting a voice of protest. Fortunately, the door cannot be closed at this point, despite opposition. Cyberdemocracy has provided for this opportunity and as it continues to expand in places like the Middle East, its impact can no longer be overlooked.

References

Africa Internet Facebook usage and population statistics. Internet World Stats: usage and population statistics, 8 Mar 2013. http://www.internetworldstats.com/africa.htm. Accessed 16 Apr 2013

Allagui I (2009) Multiple mirrors of the Arab digital gap. Global Media J 8(14). http://lass.purdue.edu/cca/gmj/sp09/gmj-sp09-allagui.htm. Accessed 15 Apr 2013

Bakr N (2012) The Egyptian revolution. Change and opportunities in the emerging Mediterranean. Gutenberg, Malta, pp 57–81, http://www.um.edu.mt/__data/assets/pdf_file/0004/150394/Chapter_4_-_Noha_Bakr.pdf. Accessed 15 Apr 2013

Campbell DFJ, Carayannis EG (2013) Epistemic governance in higher education. Quality enhancement of universities for development (SpringerBriefs in Business). Springer, New York, NY, http://www.springer.com/business+%26+management/organization/book/978-1-4614-4417-6

Campbell DFJ, Barth TD, Pölzlbauer P, Pölzlbauer G (2012) Democracy ranking (edition 2012): the quality of democracy in the world. Democracy Ranking (Books on Demand), Vienna, http://www.amazon.com/Democracy-Ranking-Edition-David-Campbell/dp/3848217988/ref=sr_1_22?ie=UTF8&qid=1349340296&sr=8-22&keywords=Campbell%2C+David+F+J and http://www.amazon.com/Democracy-Ranking-Edition-2012-ebook/dp/B009KVQ19E/ref=sr_1_12?ie=UTF8&qid=1349346706&sr=8-12&keywords=Campbell%2C+David+F+J and http://www.amazon.de/Democracy-Ranking-Edition-2012-Quality/dp/3848217988/ref=sr_1_6?ie=UTF8&qid=1357199668&sr=8-6

Carayannis EG, Campbell DFJ (2012) Mode 3 knowledge production in quadruple helix innovation systems. 21st-Century democracy, innovation, and entrepreneurship for development (SpringerBriefs in Business). Springer, New York, NY, 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

Egypt overview. Countries. World Bank, Apr 2013. http://www.worldbank.org/en/country/egypt/overview. Accessed 17 Jun 2013

Egypt court bans all Muslim brotherhood activities nationwide. RT.com. 23 Sept 2013. http://rt.com/news/egypt-court-muslim-brotherhood-235/. Accessed 16 Oct 2013

El-Erian MA (24 May 2013). Revolution 2.0 – how one Google exec Facebook sparked an uprising in Egypt. The Huffington Post. http://www.huffingtonpost.com/mohamed-a-elerian/revolution-20-how-one-goo_b_3333340.html. Accessed 17 Jun 2013

De Soto H (16 Dec 2011) The real Mohamed Bouazizi. Foreign Policy Magazine. http://www.foreignpolicy.com/articles/2011/12/16/the_real_mohamed_bouazizi. Accessed 17 Jun 2013

Facebook – about. Facebook. https://www.facebook.com/facebook/info. Accessed 17 Apr 2013

Fahim K (21 Nov 2012) Bahrain failed to deliver promised changes, report says. The New York Times. http://www.nytimes.com/2012/11/21/world/middleeast/bahrain-didnt-enact-promised-changes-report-says.html?ref=bahrain. Accessed 17 Apr 2013

Gall C (28 Sept 2013) Islamist party in Tunisia to step down. New York Times. http://www.nytimes.com/2013/09/29/world/africa/islamist-party-in-tunisia-to-step-down.html?_r=1&. Accessed 28 Sept 2013

Hofheinz A (2007) Arab Internet use: popular trends and public impact. In: Sakr N (ed) Arab media and political renewal: community, legitimacy and public life. I.B. Tauris, London, pp 56–75

Hofheinz A (2011) The Arab spring. Nextopia? Beyond revolution 2.0. Int J Commun 5: 1417–1434, ijoc.org/ojs/index.php/ijoc/article/viewfile/1186/629. Accessed 15 Apr 2013

Litvak M (2011) Iran: prospects and obstacles to democratization. In: The causes and consequences of democracy: regional and global perspectives. Tel Aviv: Stanford University Department of Political Science; Moshe Dayan Center for Middle Eastern and African Studies Tel Aviv University, pp 1–13. https://politicalscience.stanford.edu/causes-and-consequences-democracy. Accessed 16 Apr 2013

Lynch M (7 Feb 2013) Twitter devolutions: how social media is hurting the Arab spring. Foreign Policy Magazine. http://www.foreignpolicy.com/articles/2013/02/07/twitter_devolutions_arab_spring_social_media. Accessed 16 Oct 2013

Körner K, Masetti O, Forster M, Friedman J (2013) Two years of Arab spring where are we now? What's next? In: Lanzeni ML (ed) Current issues: emerging markets. Deutsche Bank AG, DB Research, Frankfurt, pp 1–14, http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PROD0000000000300328.PDF. Accessed 17 Sept 2013

Middle East Internet usage statistics, population, Facebook and telecommunications reports. Internet World Stats: usage and population stats, 2012. http://www.internetworldstats.com/stats5.htm. Accessed 16 Apr 2013

Middle East Internet usage stats and Facebook statistics. Internet World Stats: usage and population statistics, 9 Jan 2013. http://www.internetworldstats.com/middle.htm. Accessed 16 Apr 2013

Mourtada R, Salem F (2012) Social media in the Arab world: influencing societal and cultural change? In: Arab social media report 2.1 (2012) The fourth Arab social media report: influencing societal and cultural change? Dubai School of Government, pp 1–29. http://dsg.ae/en/publication/Description.aspx?PubID=306&PrimenuID=11&mnu=Pri. Accessed 28 Apr 2013

Rifaat Y (2008) Blogging the body: the case of Egypt. Surfacing 1(1):51–71, The American University in Cairo. http://www.aucegypt.edu/GAPP/IGWS/GRADCENT/Pages/Surfacing.aspx. Accessed 15 Apr 2013

Salvatore A (2011) Before (and after) the 'Arab spring': from connectedness to mobilization in the public sphere. Orient Modern 1:5–12, Academia.edu. http://www.academia.edu/1416964/Before_and_After_the_Arab_Spring_From_Connectedness_to_Mobilization_in_the_Public_Sphere. Accessed 17 Apr 2013

Steiman D (2012) Military decision-making during the Arab spring. In: Democracy & society 9.2:1–31. Georgetown University. http://www.democracyandsociety.com/blog/wp-content/uploads/2012/05/DS.pdf. Accessed 20 Apr 2013

St-Louis H (2010) Iranian political unrest in cyberspace. Democr Soc Democrat Dictator Demostrat Conf 7(1):2–4, D&S Vol. 7 Iss. 2 Spring 2010. Georgetown University. The Center for Democracy and Civil Society. http://www.democracyandsociety.com/blog/democracy-society-journal/ds-vol-7-iss-2-spring-2010/. Accessed 25 Apr 2013

Transcript – Charlie Rose interviews Bashar Al-Assad. 10 Sept 2013. http://www.scribd.com/doc/166980913/Transcript-Charlie-Rose-Interviews-Bashar-Al-Assad. Accessed 15 Sept 2013

Trew B (6 June 2013) Egypt's Khaled said: three years on, still no justice. In: Ahram Online http://english.ahram.org.eg/NewsContentP/1/73310/Egypt/Egypts-Khaled-Said-Three-years-on,-still-no-justic.aspx. Accessed 17 Jun 2013

Twitter – about. Twitter. https://twitter.com/about. Accessed 25 Apr 2013

UAE places restrictions on online dissent. BBC News. 13 Nov 2012. http://www.bbc.co.uk/news/world-middle-east-20317803. Accessed 17 Jun 2013

Zarwan E, Goldstein E, Stork J, PoKempner D, Saunders J (2005) False freedom online censorship in the Middle East and North Africa. Human Rights Watch 17.10E(2008):1–144, http://www.hrw.org/sites/default/files/reports/mena1105webwcover.pdf. Accessed 20 Apr 2013

Chapter 6
Democratization in the Middle East and North Africa: Tunisia, Egypt, and Turkey

Tuğba Özcan

Abstract This chapter deals with the question of democratization in the Middle East and North Africa in recent years. The chosen examples are Tunisia and Egypt as examples 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 chapter is given to the role of new media in the protests for and the process of democratization.

Keywords Arab Spring • Democratization • Egypt • Middle East • North Africa • Revolution • Social Media • Tunisia • Turkey

6.1 The Process of Democratization in Tunisia and Egypt

6.1.1 Introduction

"The Arab Spring is a historical turning point in the region entailing widespread political, economical and geostrategical consequences."[1]

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.

[1] Cited after Kreft (2011)

T. Özcan (✉)
Master Studentin in Universität Wien, Vienna, Austria
e-mail: tuba_oezcan@hotmail.com

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_6,

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.[2] 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.[3]

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, but 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 non-violent 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.

6.1.1.1 Theses on the Development of the Arab Spring

- The rentier states and the allocation regimes, as well as the politics of the USA 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 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 struggled in Egypt and Tunisia, or they lead to 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.

[2] 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."

[3] See Kreft (2011)

- 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 Taher Ben Jelloun's hope that "never again a dictator will be able to stomp on the dignity of the Arabic people,"[4] 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 one hundred years ago is pertinent: "Socialism or Barbarism!"[5]

6.1.2 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

[4] Preiss (2013), cited after Ben Jelloun (2011), p.91

[5] Preiss (2013), p.221 cf.

bureaucratic apparatus and generally a large overblown security apparatus as well, which is supported by foreign help. Wolfgang Muno[6]: "Without a tax system there is no mutual dependence between the citizens and the state ('no taxation without representation')."[7] 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.

"Dr. Muno sketches and displays the different stages of democracy 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)"[8]

Many of the affected countries, says Muno, are very young: 65-75 % of the population is 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."[9]

6.1.3 Revolution

After the Tunisian President Zine el-Abidine Ben Ali had to flee the country in a hurry after week-long protests on January 14th 2011, the successful revolution in Tunisia became an inspiration for the anger that has been brewing under the surface

[6] Cited after Mainz (2012)

[7] Ebd.

[8] Cited after ibid.

[9] Cited after ibid.

in Egypt for years. The European and US-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 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,[10] 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."[11]

[10] Preiss (2013); see Todd (2011)

[11] Teorell (2010), cited after Preiss (2013), 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 US-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, but 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.[12]

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; and
- *Sanctions*, punishments, threatened or applied, against the disobedient and non cooperative to ensure the submission and cooperation that are needed for the regime to exist and carry out its policies."[13]

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, that is to provide economic and social security, which can be 'traded' for political freedoms.

[12] Sharp (2010), cited after Preiss (2013), p.67.

[13] Sharp (2010), cited after Preiss (2013), p.18f.

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 he Egyptian state remained largely untouched, while the regimes were overthrown or transformed.[14]

6.1.3.1 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 amongst the best educated in Northern Africa. Yet the economy tended to create jobs mostly for unskilled workers and in the low-wage sector. Unemployment amongst academics is at 35 % and thus almost twice as high as amongst 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 led to a massive decrease in tourism at the Mediterranean coast.[15]

6.1.3.2 The Egyptian Revolution

In Egypt, the political change is very often described as a military coup d'état. 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

[14] See Preiss (2013), p.207

[15] See Pott (2012), p.124

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.[16]

6.1.4 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, but 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.”[17] If 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.

[16] See Preiss (2013), p.34

[17] El-Gawahry (2011), cited after Preiss (2013)

6.1.5 *Is a Democratic Development Possible?*

In Egypt and Tunisia a development towards 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 al-Adli, 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,[18] journalists, artists, human rights activists and activists. Those criticizing the military council and calling for a continuation of the protests[19] 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 towards 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 Husni 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[20] and decision-making. Yet

[18] Cited after Preiss (2013): "Thus the military council freed Colonel Aboud al-Zomor, 'the mastermind behind the Sadat assasination,' 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)

[19] Cited after Preiss (2013): "It is said that there have already been 5000 people sentenced by military courts, says Amira El Ahl (2011) 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

[20] Erhardt (2011)

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*,[21] but the party does not want to found 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."[22] 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) Muhammed Badie, the leader of the Muslim Brotherhood, declared as the goal 50 % of the seats in parliament and the introduction of Sharia law.[23] 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 Rashid al-Ghannushi, living in exile in London for a long time and the founder of the Islamist En-Nahda-Movement, returned to Tunisia. Al-Ghannushi is a colorful personality, who on the one hand praises the Ghihadist 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."[24]

[21] See Croiteru (2011), p.87

[22] Preiss (2013) cited after Gerlach (2011), p.87

[23] See Windfuhr (2011)

[24] Ghannouchi (2011). Cited after Preiss (2013), p.86

6.1.6 *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 towards 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 amongst 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 Husni Mubarak changed many things: In both countries there is independent media; we witness a lively political debate between Islamists and Secularists, between Conservatives and Liberals about a new constitution.

There is a widespread consensus amongst 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 socio-economic 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, 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 is 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.[25]

6.1.7 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.[26]

"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."[27] "There are also those voices, however, who warn of being to quick to judge and who point to different factors of political change."[28] 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.[29]

[25] See Kreft (2011)

[26] See Milz (2012)

[27] Cited after Kneuer and Demmelhuber (2012)

[28] Cited after Kneuer and Demmelhuber (2012); Rafal: Liberations. Control in Cyberspace, in: Journal of Democracy 4/2010, p.43–58.

[29] See Kneuer and Demmelhuber (2012)

6.1.7.1 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 Bouzizi 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 %.[30]

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,"[31] 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.[32]

6.1.7.2 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."[33] 25.9 million users

[30] See Spiegel et al. (2013)

[31] Cited after Spiegel et al. (2013)

[32] See Spiegel et al. (2013)

[33] Cited after Spiegel et al. (2013)

equal roughly 30 % of the population. One and a half years before 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 1,500 bloggers. With Facebook and Twitter the number of net activists rose to some 1.5 million.[34]

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.[35]

"Even a deactivation of the internet did not hinder the use of social networks. After the internet was deactivated in Egypt Telcomix net activists spread phone numbers via fax, with which one could log on to the internet via the phone cable and provided modem pools."[36] 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.[37]

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.[38]

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.[39]

---

[34] See (Fathy (2011)

[35] See Ibd.

[36] Cited after Spiegel et al. (2013)

[37] Cited after Spiegel et al. (2013)

[38] See Spiegel et al. (2013)

[39] See Milz (2012)

If there is a great will to protest in the public, digital media are able to connect mobilized citizens quicker and more effectively, 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.[40]

6.1.8 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.[41]

6.2 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.[42]

[40] See Ibd.

[41] Lüders (2011), p.42f.

[42] 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.[43]

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.[44]

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.[45]

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.[46]

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

[43] See Schimm (2013)

[44] See Gül (2004)

[45] See Schulz (2011)

[46] See Schulz (2011)

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.[47]

6.2.1 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 Premier 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[48]: 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 towards 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.[49] Furthermore, Egypt

[47] See Schimm (2013)

[48] See Erdogan (2011a)

[49] See Erdoğan, Egypt's Muslim Brotherhood criticizes Erdoğan's call for a secular state (2011b)

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,[50] 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 towards 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, towards systems that are authoritarian and dominated by the army.[51]

6.2.2 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 are still lacking internal democracy and a liberal debate culture.

The Arab countries longing for change and modernization are however closely eying Turkey's steps towards 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.[52]

References

Ahl AE (2011) Die revolution zuerst. DIE WELT 7

Croiteru J (2011) Ägyptens Muslime werben im Christen(die Beschreibung der Parteiverfassung). FAZ S. 35

[50] See Orient-Institut (2011)

[51] See Schulz (2011)

[52] See Schulz (2011)

Cynthia F (2011) The Arab upheaaval: Egypt's Islamist shadow. Von the Middle East quarterly. 18/3:S.35. www.meforum.org/2887/arab-upheaval-egypt-islamist abgerufen.
Ehrhardt C. Aktivismus in Zeiten der Verunsicherung. FAZ. 2011:S. 1.
El-Gawahry K (2011) Tagebuch der arabischen revolution. Kremayr& Scheriau, Wien
Erdogan RT (2011) "Turkey's Erdogan tells Arabs to embrace democracy." vor der Arabischen Liga und der Generalversammlung der Vereinten Nationen. Vereinigten Nationen. http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=19021&catid=74&Itemid=30
Erdogan RT (2011) "Egypt's Muslim Brotherhood criticizes Erdogan's call for a secular state". Ägypten: news. www.alarabiya.net/articles/2011/09/14/166814.html
Fathy B (2011) 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
Gerlach J (2011) 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
Ghannouchi R (2011) "Jeder soll entscheiden, was er trägt". FAZ S. 6
Gül A (2004) Turkey's role in a changing Middle East environment (S. 1–7). Middle East quarterly
Jelloun TB (2011) Arabischer Frühling:vom Wiedererlangen der arabischen Würde. Berlin Verlag, Berlin
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.politisch-ebildung.com/pdfs/35kneuer.pdf
Kreft H (2011) 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. C.H. Beck oHG, München
Mainz EH (2012) Abgerufen am 04. 01 2013 von Konrad Adenauer Stiftung. http://www.kas.de/wf/doc/kas_30185-1522-1-30.pdf
Milz K (2012) 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. Kiepenheuer & Witsch, Köln
Preiss B (2013) Zeitenwende im Arabischen Raum. LIT Verlag, Wien
Schimm M (2013) 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) 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. Fourth U.S. Edition, East Boston
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
Todd E (2011) Frei! Der arabische Frühling und was er für die Welt bedeutet. Piper Verlag, München
Windfuhr V (2011) Nach der Revolution: Ägypten erfindet sich neu. Abgerufen am 17. 8 2011 Spiegel-Verlag, www.spiegel.de. Das Nachrichtenportal im Internet, Hamburg

Chapter 7
Cyber Democracy: The Future of Democracy?

Thorsten D. Barth and Willi Schlegelmilch

Abstract *Is a Cyber Democracy the future of a democratic society*? Always new scandals from the virtual world, also known as 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. With the perspective of today it seems almost impossible to ensure the needed security levels, which a Cyber Democracy would require for the participation, the competition, the freedom and the equality in the virtual world of the Internet. Following this a Cyber Democracy appears at this point in time not to be the future of democracies. However, the 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. 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.

Keywords Democracy • Cyber democracy • Cyberspace • Democratic society • Quality of democracy

T.D. Barth (✉)
Vienna, Austria
e-mail: thorsten.d.barth@gmail.com

W. Schlegelmilch, M.B.A.
Schönaich, Germany
e-mail: CWSchlegelmilch@t-online.de

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_7,

7.1 Introduction

Our world is undergoing change. This change will have negative as well as positive impact. It is also a fact that this change and the related transformation processes will come together with major challenges. 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. Never until now during the known history of mankind was it so easy to communicate globally and to share information so rapidly. Looking with this in mind to the democratic countries it becomes clear, that the democratic societies of the western world have to be modernised, when they want to survive as functioning political democratic systems in the already existing digital environment but even more in the digital era of the future. With this article we therefore ask the question: *Is a Cyber Democracy the future of a democratic society*?

Always new scandals from the virtual world, also known as 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. With the perspective of today it seems almost impossible to ensure the needed security levels, which a Cyber Democracy would require for the participation, the competition, the freedom and the equality in the virtual world of the Internet. Following this a Cyber Democracy appears at this point in time not to be the future of democracies. However, the 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. 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.

7.2 Democracy, Cyberspace and Cyber Democracy: What Does It Mean?

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 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 article and following Abraham Lincoln, democracy shall be understood as “government of the people, by the people, and for the people” (quote from Lincoln and Chittenden 2009, p. 133). 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, 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, for example, Campbell and Barth 2009; Diamond and Morlino 2005; Barth 2011).

For the definition of democracy we therefore want to give an empirical overview about the current developments regarding the quality of democracy based on a global comparison for 2012. This comparison is based on the Democracy Rankings[1] conducted by the independent democratic research initiative (see Fig. 7.1, World Map).

The figures show that when classifying the democracies in a range from *very high quality* to *very low quality* 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* or *very low quality of democracy* or even *dictatorial quality*.

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, for example, 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),

[1] The Democracy Ranking is an annual study of democracy (see, Campbell et al. 2012), 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". Although the Russian Federation, Yemen, China, Egypt, Libya, Tunisia and Syria were classified by Freedom House as "not free" they were integrated from the year 2012 as exceptions in the new ranking of 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 analyse 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. Initiator of this project is Sàndor Hasenöhrl, an entrepreneur from the computer and software industry (read more on: www.democracyranking.org).

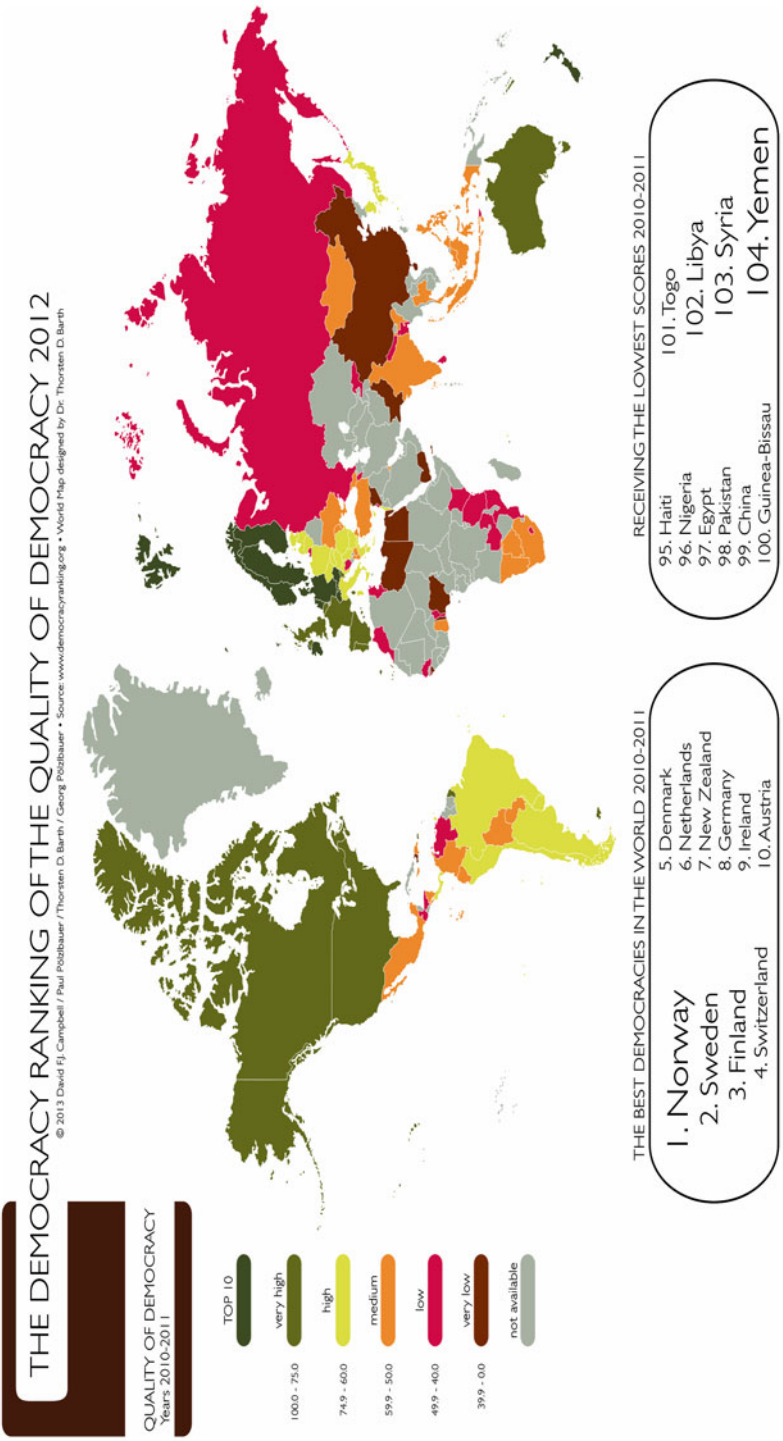

Fig. 7.1 World map of the democracy ranking 2012

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 characterised 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

Cyberspace can be understood as an artificial word composed of *cyber* representing the "cybernetics" and *space* as short form representing the "universe" or the "outer space". Based on this the Cyberspace can be seen as the "cybernetical universe." By contrast to the "outer space" the Cyberspace is hereby regarded as technical term and defined as room for data. In the context of Cyberspace the definition of democracy as Cyber Democracy must now be given. The term "Cyber Democracy" itself contains a broad range of content and definitions. 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. 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 for example the E-Democracy, are very often connected with technological innovations and the future of democracy (see Campbell 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).

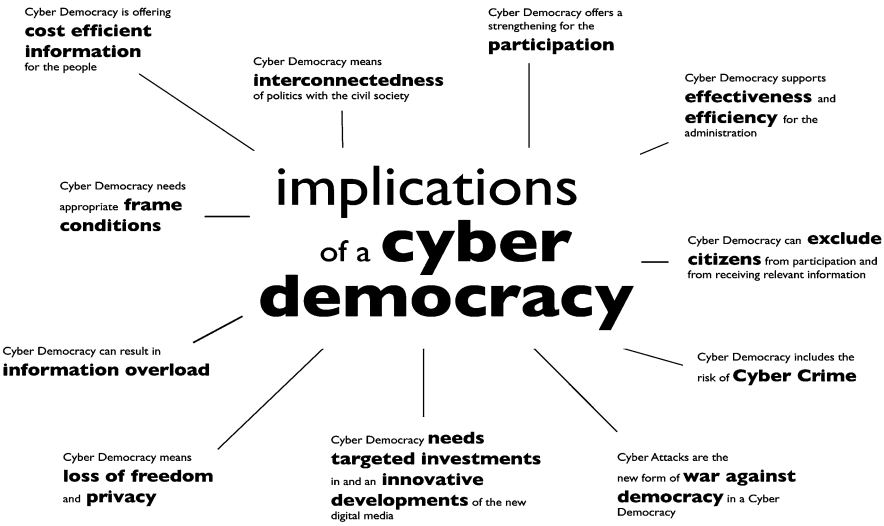

Fig. 7.2 Implications of a cyber democracy

7.3 Discussion: What Are the Implications of a Cyber Democracy?

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 summarised as well as the related chances and risks (see Fig. 7.2):

7.3.1 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 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.

7.3.2 Cyber Democracy Needs Targeted Investments in Innovative Developments 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. Therefore this implies big investments by the states willing to develop in this direction as well as necessary innovative achievements by these states.

7.3.3 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 over informed and following this less informed citizen.

7.3.4 Cyber Democracy Offers a Strengthening for the 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.

7.3.5 Cyber Democracy Can Exclude Citizens from Participation and from 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) use the term “information elites”. Even if it is that the majority of the people in a democratic and modern society own 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.

7.3.6 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.

7.3.7 Cyber Democracy Includes the Risk of Cyber Crime

Together with the digitalisation 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.

7.3.8 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, were 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.

7.3.9 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.

7.3.10 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.

7.3.11 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 has become a lot easier, but the digital human being is fully transparent and must be aware about his loss of freedom and privacy.

7.4 Conclusion

In this article we raised the question, whether a Cyber Democracy will be the future of our democracy. As a summary after evaluating the chances and the risks it becomes clear, that at this point in time in the year 2013 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 transmitting, sharing and collecting information. A Cyber Democracy supporting and executing direct democratic decisions and operating direct democratic processes can at this point in time only be declined. The main reason being, 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 wire-tap 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 2 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.

Our statement therefore is that the risks resulting from a Cyber Democracy are predominant and as well not 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 modernisation of democratic systems (see, for example, Carayannis et al. 2012). This modernisation is however also needed for the current democratic societies and can be summarised with the following five points (see Fig. 7.3):

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.

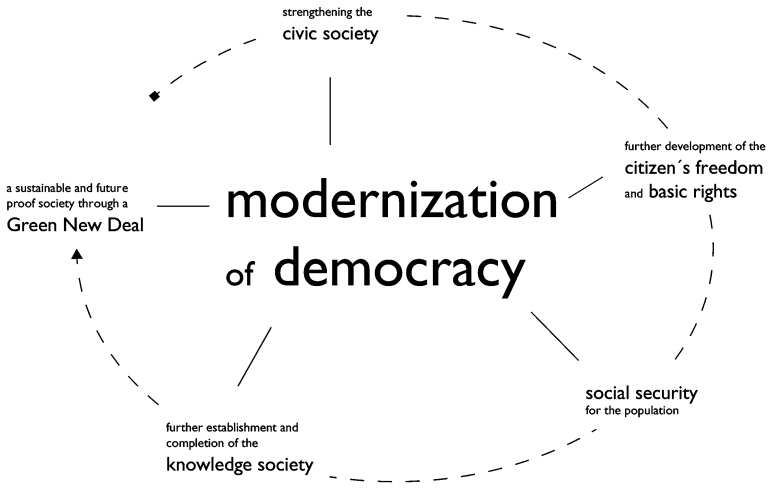

Fig. 7.3 Modernisation of democracy

7.5 Cross-References

Knowledge Society, Democracy of Knowledge, Quintuple Helix

References

Barth TD (2011) The idea of a green new deal in a Quintuple Helix Model of knowledge, know-how and innovation. Int J Soc Ecol Sustain Dev 2(1) (http://www.igi-global.com/article/idea-green-new-deal-quintuple/51633)

Barth TD (2013) Freedom, equality and the quality of democracy: democratic life in the United States, Australia, Sweden and Germany. Int J Soc Ecol Sustain Dev 4(1) (http://www.igi-global.com/article/freedom-equality-quality-democracy/77345)

Campbell DFJ, Barth TD (2009) Wie können Demokratie und Demokratiequalität gemessen werden? Modelle, Demokratie-Indices und Länderbeispiele im globalen Vergleich. SWS-Rundschau 49(2):208–233 (http://www.uni-klu.ac.at/wiho/downloads/campbell_u._barth-demokratiemessung-sws_rundschau-heft_2009_02-FINAL.pdf)

Campbell DFJ, Pölzlbauer P, Barth TD, Pölzlbauer G (2012) Democracy ranking 2012: the quality of democracy in the World: method and ranking outcome. Comprehensive scores and scores for the dimensions. Democracy ranking, Vienna. (http://democracyranking.org/wordpress/?page_id=392)

Carayannis EG, Barth TD, Campbell DFJ (2012) The Quintuple Helix Innovation Model: global warming as a challenge and driver for innovation. J Energ Innovat Enterpren 1(1):1–12 (http://www.innovation-entrepreneurship.com/content/pdf/2192-5372-1-2.pdf)

Diamond L, Morlino L (2005) Introduction, ix–xliii. In: Diamond L, Morlino L (eds) Assessing the quality of democracy. The John Hopkins University Press, Baltimore, MD

Peter F (2003) Chapter 21—cyber-democracy. In: Axtmann R (ed) Understanding democratic politics: an introduction. SAGE, Thousand Oaks, CA, Pub. date: 2003, Online Pub. Date: May 31, 2012. doi:10.4135/9781446220962. Print ISBN: 9780761971832. Online ISBN: 9781446220962

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 LE (2009) Abraham Lincoln's speeches. General Books (http://www.booksamillion.com/p/Abraham-Lincolns-Speeches/Abraham-Lincoln/9781175395603)

O'Donnell G (2004) Human development, human rights, and democracy, 9–92. In: O'Donnell G, Cullell JV, Iazzetta OM (eds) The quality of democracy. Theory and applications. University of Notre Dame Press, Notre Dame, IN

Chapter 8
Cyber-Democracy and Cybercrime: Two Sides of the Same Coin

Birgit Mitterlehner

Where is the Life we have lost in living?
Where is the wisdom we have lost in knowledge?
Where is the knowledge we have lost in information?

T.S. Eliot

Abstract The 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. This chapter assesses potential advantages and risks in knowledge societies in terms of cyber-democracy and cybercrime.

Keywords Cyber-democracy • Cybercrime • Cyber-governance • Bring your own device (BYOD) • Cloud computing • Consumerization of IT • CoIT • Private cloud • Public cloud • Knowledge worker • Workplace democracy

8.1 Introduction

Networking opportunities and possibilities for interaction and communication have increased as the pace of emerging ICT technologies has spurred. As a result, the volume of codified knowledge has cumulated and the possibilities to access knowledge at any time and place have significantly improved.

While on the one hand, these developments have enlarged the potential for a sound knowledge democracy to be established, they may constitute a new source for cybercrime on the other. This is particularly so when it comes to knowledge produced

B. Mitterlehner (✉)
Außeruniversitäres Institut Public Social, Responsibility gemeinnützige Gesellschaft mbH, Annagasse 6, 1010 Vienna, Austria
e-mail: birgit.mitterlehner@gmx.at

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_8,

in and by businesses, governments and public authorities. ICT blackouts (e.g. electricity networks) and data theft may have a severe impact.

Historically, the military and the industry used to be the driving forces in ICT development. Being developed for military and industrial reasons, those technologies already fulfilled certain security standards when offered to the consumer; meanwhile, consumer have become the driving forces behind ICT development. This trend is called *Consumerization of IT* (CoIT) and it has equipped the general public with powerful devices. Using these devices, they may engage in active citizenship at any place and time. CoIT has introduced multidimensional changes which require a mature security response that is risk-based and demands a high degree of sophistication.

One phenomenon which is deeply connected to CoIT is *Bring-Your-Own-Device* (BYOD). Being one of the international top security risks 2013 (Infosecurity Magazine 2012), BYOD refers to the use of professional data on private end-devices or by using public applications. This trend was made possible by the interoperability of private and professional devices and it was mainly brought about employees wishing to use their own devices and applications for work, as the frontiers between professional and private life became blurred (Dell and Intel 2011: 8). In fact, work attitudes have changed and extended old work patterns, notably with regard to higher positions and knowledge workers. Today, employees, and particularly knowledge workers, may wish or need to reach and access information independent of location and time.

Data security is being challenged not only by technical challenges but also by the existing disarray of heterogeneous rules and legislation (e.g. international data protection and contract law). Also, non-compliance constitutes an often underestimated security risk. As a result, strategies such as the Austrian ICT Security and Safety Strategy claim that it is important that uniform, standardized solutions be developed in a stakeholder dialogue in order to meet the new challenges (Digitales Österreich 2012).

This chapter assesses potential advantages and risks in knowledge societies in terms of cyber-democracy and cybercrime. It is based on a comprehensive desktop research. While assessing risks for businesses and governments, the rights and obligations of employees will be discussed, too. The research questions pursued are:

1. In which ways has Consumerization of IT influenced the potential of cyber-democracy and cybercrime?
2. How far does cyber-democracy go?
3. When does cyber-freedom affect cyber-security?—BYOD.

In order to answer these research questions, this chapter is divided into the following sub-chapters. First, a small encyclopaedia and synopsis of cyber-concepts and vital terms is meant to introduce the subject. Second, the evolution of ICT will be described. A particular emphasis is to be put on cyber-democracy and cybercrime as well as the legal challenges connected to a global virtual space. In this regard, the recent trend Bring-Your-Own-Device is to be discussed.

8.2 Terminology

8.2.1 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: 39; Oppliger 2011; Lennon 2012).

8.2.2 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: 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".

8.2.3 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 cyberspace 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 cyberspace are assessed in this chapter.

8.2.4 Cyberspace

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: 3f). However, this chapter particularly refers to the Internet when using the term cyberspace.

8.2.5 Cybersecurity

> "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: 2f).

This term denotes both, a status and a process targeted at the mitigation and resolution of all risks related to the cyberspace. It includes political, technical, administrative, legal and any other counter-measures to a threat. A secure cyberspace grants integrity, confidentiality, authenticity of information (ITU-T 2008).

8.2.6 Consumerization of IT (CoIT)

There are distinct definitions of CoIT. Murdoch, Harris and Devore 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: 2). Harris et al. (2011: 3) refer to this paradigm as "the adoption of consumer applications, tools and devices in the workplace". BYOD is a side-effect thereof; employees have started to revert to using their consumer applications instead of (probably more secure) business ICT-frameworks (by using iPhones, Dropbox, etc.) (Harris et al. 2011: 4ff). This chapter relates to CoIT as a process where IT is conceived in a customer-friendly and marketable way.

8.2.7 Knowledge Worker

In this chapter, knowledge worker means any staff whose main capital is knowledge. In terms of cybersecurity, it means that they have access to, use or produce explicit or documented knowledge and classified information of an organization.

8.2.8 Organization

Any business, company or organization—be it under private or public law.

8.2.9 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).

8.2.10 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).

8.2.11 Risk

A "Threat which abuses vulnerabilities of assets to generate harm for the organization" (ISO/IEC 27005).

8.3 Towards Consumerization of IT

Among other factors, the era of globalization has been characterized by the democratization of technology and information according to Friedman (1999). The fact that ICT is being used by everybody for even mundane activities has its origins in a change in the IT innovation paradigm (Moore 2011; Niehaves et al. 2012; Harris et al. 2011) which took place in the course of the last decades:

In the beginnings of ICT development, the military and the industry used to be in charge. Only after having been successfully conceived and implemented was ICT made available to the consumer. As a consequence, information and communication technologies would meet certain security standards automatically.[1] This process has been inversed. As the pace of ICT innovation increased, public demand increased, too, and mass production led to affordable prices so that by now, consumers have become the driving force behind technological developments in the telecommunications industry (Harris et al. 2011: 2ff). This commercialisation of IT is popularly referred to as Consumerization of IT (CoIT) (Baskerville 2011: 251ff). It has empowered those outside of the technical industry to access, use and possess

[1] However, when the cyberspace was "constructed", major security aspects were neglected so that it would be wrong to say that there were no security risks if ICT had not become consumerized.

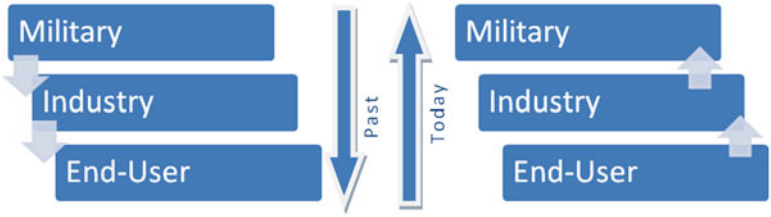

Fig. 8.1 Paradigm shift in ICT development [made by author]

powerful and user-friendly ICT products and applications (Moschella et al. 2004: 12; Choucri 2000: 248–252). As a result, the cyberspace has turned into a multidimensional platform of action (of several million websites) where information may constantly be created, processed and modified (=knowledge creation) (Choucri 2000). Figure 8.1 summarizes this trend:

Examples of CoIT include, but are not limited to:

- IPhone
- Tablet PCs
- Android smartphones
- MP3 Player
- Google (e.g. Drive, Calendar, Mail, Apps) (Clouds)
- Dropbox (Cloud)
- Microsoft SkyDrive
- OwnCloud
- CloudME
- Ubuntu One
- CloudSafe
- Facebook
- …

Per definition, services of general (economic) interest are fundamental services and, as such, have become an integral part to a society. Thanks to CoIT, ICTs and the cyberspace have come to be understood as such a service of general (economic) interest (Mitterlehner and Barth 2013; Mitterlehner 2013). In accordance with the Charter of Fundamental Rights of the European Union, they ought to, therefore, be available to the general public at affordable prices and be of commensurate quality (CFR: Art. 36; TFEU: Protocol 26). As such, the Internet as a decentralized communication system has become a cornerstone for the information and knowledge-society and changed society as profoundly as the printing press did (Leiner et al. 1997). Accordingly, the European Union even pursues special policies to foster the use, access and security in the cyberspace (Digital Agenda 2010).

In the past, numerous scientists claimed that the cyberspace would enlarge the information gap within and between societies due to a gap in ICT-literate and non-literate persons (digital divide) (Benton Foundation 1998; DiMaggio and Eszter 2001).

Even though there still is a digital gap between the haves and the have-nots in terms of access and usage (Hammond 2001; Choucri 2000; Chen and Wellman 2005), those fears have proven unfounded in the industrialized countries, and even more so when it comes to the digital generation and the generations that are to come (Chen and Wellman 2005). In fact, certain inequalities notwithstanding, the existing digital gap has been decreasing in Europe (Eurostat 2013). The pace of cyber-development and technological innovation have boosted access to the cyberspace and created new ways of knowledge production, access and sharing (i.e. social networking, chatting, blogging or virtual teams) (ENISA 2012b; Castells and Cardoso 2005: 13ff).

To sum up, the cyberspace has become a fundamental service and an integral part of today's knowledge society. However, the security risks connected to the cyberspace have multiplied as the Internet became commercialized in the 1990s. As a result of CoIT and market pressure, providers of consumer devices and public applications may neglect security standards beyond legal standards as security does not trigger higher profits. In fact, security standards may even be to the detriment of functionality and intuitivity. Since the development of security measures is a lengthy process, it may even prove more time-efficient for them to release a new generation of devices or application (Cavelty 2012).

8.4 Cyber-Democracy vs. Cybersecurity in the Cyberspace

The Internet has added a cyber-dimension to our society. Besides CoIT having supplemented traditional action patterns such as posting letters, shopping, and paying bills online, the malleability of ICT offers numerous innovative communication possibilities (Papacharissi 2010). On the one hand, they have equipped (notably the Western) society with a plethora of devices (democratization of technology) (Sambharya et al. 2005) with which to access the Internet at any place and time.[2] On the other hand, the Internet's folding into existing social functions and extending them in new ways[3] has clearly challenged the concepts of the public, the professional and the private sphere as well as the modes of participation and ways of interaction in either of them (Poster 1995).

While Web 1.0 enlarged the potential for the knowledge society and extended traditional forms of dialogue (top-bottom), Web 2.0 may re-configure communicative power relations and bring about a more inclusive democracy. This "new" framework structure has given people a voice (bottom-up, horizontal communication) regardless from their place, their condition (tied to a hospital bed) or their cultural,

[2] While the cyberspace offers everybody using it a democratic voice, it is not by itself inherently democratic. Instead, it is dominated by a few giant applications such as Google, Facebook and YouTube. Also search engines rank algorithms and therefore privilege access to certain information (Halavias 2009). As such a "disproportionate authoritative influence over information sources" is being produced (Loader and Mercea 2011). Yet this shall not be subject to discussion here.

[3] Brought about by CoIT and the democratization of IT that goes hand in hand with it.

linguistic or ethnic background. These social functions have also challenged the concept of the political arena and existing theoretical approaches and concepts of democracy (Klein et al. 1999): Users do not have to be passive consumers, but they may challenge "the monopoly control of media production and dissemination by state and commercial institutions" by sharing alternative perspectives and publishing their own opinions (Loader and Mercea 2011; Papacharissi 2010).

In the last years, political efforts have been targeted at the cyberspace and the implementation of cyber-democracy in order to revive or enhance political participation and dialogue (compare: Digital City Amsterdam, etc.) (Klein et al. 1999), for it offers a platform for the exchange of opinions and ideas in (a)synchronical ways regardless of space and time (Klein et al. 1999). By way of example, the Pirate Party Movement in Europe is one of the most shining examples of how the cyberspace and the digital generation may upset "traditional" forms of democracy (Lewitzki 2011). It has introduced a multifaceted digitalized Internet-based participation process:

Their Wiki and their forum are internally and externally accessible platforms for discussion. Social media such as Twitter and blogs serve the purpose of being present and recognized in the political arena. Their LiquidFeedback is probably the most interesting tool, since it is supposed to implement a form of liquid democracy as they call it. In fact, it is a tool to further develop their party program in a participatory way. Everybody (even non-members) may put their ideas on the agenda and, depending on how they are received by the community, they will be pursued or put on the back burner. Even if the Pirate Party Movement also holds non-virtual meetings, 90 % of their communication takes place online (Lewitzki 2011: 17). In this regard, the Pirate Party Movement may be the first political movement fully exploiting the potential of cyber-democracy. This may go so far as to virtually exclude non-digitally literate or digitally fluent people.

Yet the acquisition of a tablet, a smartphone or a laptop does not entail political participation, even if, in theory, it enhances possibilities of democratic participation and active citizenship (by means of forums, blogs, e-voting, etc.) or at least 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 (Rettberg 2008). Therefore, it has provoked controversy if cyber-democracy is apt to meet today's problems such as disenchantment with politics and allows for reaching groups beyond those who are committed democratic participants (Castells and Cardoso 2005). Besides questions about 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: 563).

The controversial opinions on this issue notwithstanding, it is likely that the cyberspace may have at least a certain positive impact, notably among younger generations (see: Loader and Mercea 2011; Baron 2008; Brandtzaeg et al. 2009; Livingstone et al. 2011; Dahlgren 2003). A recent study on the role of the Internet

in German elections also underlined that the cyberspace does occupy an important role for democracy (BITKOM 2013). Therefore, even if the "democratizing effect" of the cyberspace cannot be proven, there is no need to adopt another line of reasoning.

Finally, the discussion on cyber-democracy should not be limited to traditional forms of democracy such as (e-)voting. With regard to the democratic power of the cyberspace, a wider approach of democracy and democratic participation (which surpasses voting, party membership, petitioning representatives) ought to be applied. 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[4] (Campbell and Barth 2009).

8.4.1 The Variables Information and Knowledge in Cyber-Democracy

Agenda-setting and awareness-raising are crucial for the political realm. The cyberspace has challenged processes of information distribution and knowledge creation, dissemination and processing. Therefore, cyber-democracy is assessed from the angle of information and knowledge[5] in this sub-chapter.

With regard to knowledge societies, (Nowotny et al. 2003; Etzkowitz and Leydesdorff 2000; Etzkowitz 2002; Carayannis and Campbell 2009) have developed models which describe different modes of knowledge creation and knowledge processing, whereby the most advanced ones (featuring Western democracies) are based on the understanding that different spheres of action (academia, state, industry (media, sustainability), etc.) interact in a way helices do (Gibbons et al. 1994; Etzkowitz and Leydesdorff 2000; Carayannis and Campbell 2009; Carayannis and Campbell 2010). As outlined in their helix models, knowledge creation and processing may take different forms. Particularly, the quadruple and quintuple helix models show how interdependent spheres become when knowledge circulates (knowledge input and knowledge output) freely (Barth 2011). Where quadruple and quintuple

[4] The majority of democracy measurements include, besides other factors, education.

[5] The different models in knowledge management as well as the differences in knowledge or between knowledge and information shall not be referred to, here. For more information on this, see Kettinger and Li (2010); Capurro (2005); and Canals, Agustí (2004). Sound definitions are also provided in D-A-CH Wissensmanagement Glossar (2010).

helix modes (as conceived by Carayannis and Campbell 2010; Carayannis et al. 2012) exist, they create nourishing ground for knowledge societies and knowledge democracy. The cyberspace may be viewed as a pivotal instrument for knowledge democracy. As Loader and Mercea point out, the increasing ICT competence and ICT literacy (also due to the integration of ICT in our mundane activities) may have an impact on awareness-raising (e.g. transnational policies), agenda-setting and social relations of powers (e.g. Arabian spring) and, as such, on society.

8.4.2 Disruptive Actions and Expressions of Discontent: Democratic action or Security Risk?

According to Coleman and Blumler, democratic action is more than just voting and it is independent from party membership. They view the cyberspace as "an empty space or institutional void in which tensions between state-centric and democratic citizenship can be played out" (Coleman and Blumler 2009: 7). Therefore, it is proposed that the discussion shall not revolve around a potential divide between those who have gained knowledge by means of education and those who have not. Instead, it is assumed that each single piece of content in the cyberspace is information and may be transformed into tangible knowledge and, as such, be used by the empowered citizen. In this regard, the multifaceted forms of information must be given the same attention when reviving democratic action and assessing popular beliefs—be it YouTube content, blogs, newspapers, academic research, etc. Coleman and Blumler support this view; they point to the variable of "critical citizenship and radical energy" as a form of democratic citizenship (Coleman and Blumler 2009: 3).

As a consequence, it may be assumed that virtually any form of expression in any of the different spheres of action, even the explicitly non-political and expressions of discontent, is part of democratic citizenship. Using this wide definition of democracy, disruptive activities and the expression of discontent (YouTube videos, protest music, blogs) are actions of democratic citizenship, too (Loader and Mercea 2011).

However, it is difficult to draw the line between cyber-democracy and cybercrime when assessing the democratic power of expressions of discontent and disruptive activities. As information is stored electronically or in the cyberspace (in form of public or private clouds) and may be spread globally with one mouse click or smartphone click one may wonder: Which kind of expression of discontent and sharing of information may be considered democratic and which one may be considered to be a crime? This is particularly so when it comes to national security (yet also business secrets).

While granting everybody their fundamental rights of expression and participation, the sovereign (usually the state) also has to ensure national security. The polarity of this issue is 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 consequence, cyber governance has become one of the biggest challenges of our society (Eriksson and Giacomello 2006). This already starts with the question of how to protect states, businesses and citizens without infringing their freedom of expression and action. Prior to answering these questions, it is vital to draw the line between democratic citizenship, democratic empowerment and crime.

8.4.3 Implications for Practice: Bring-Your-Own-Device—A Vice or a Virtue?

Societal changes towards a knowledge economy have made the concept of work–life balance translate into work-flexibility (Maier et al. 2008; Price Waterhouse Coopers 2011: 4). Where today's work culture has shifted to working on the basis of project accountability and goal accomplishment, knowledge workers wish to access their "desks" anywhere and at any time (Entity Solutions 2013). Naturally, the spheres of privacy and work would not have intersected the way they do without CoIT having empowered the general public through affordable interoperable and compatible IT equipment. As a result of this flexibilisation, the office, the home office and the mobile office (which is everywhere) have emerged as possible work places (Martinez and Rajlkashmi 2012).

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. 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).

Within this framework of "flexibilization", the trend Bring-Your-Own-Device (BYOD)[6] has emerged. It has its origins in CoIT and means that workers use their private end-devices or privately used public applications for professional purposes. While giving them the possibility to combine private and professional life at any time and place, the use of private end-devices and applications at the workplace for professional purposes constitutes one of the international top security risks 2013 (Infosecurity Magazine 2012). As new technologies have not only provided the general public with powerful multi-dimensionally usable devices (such as smartphones, tablets, etc.) but also made those devices and applications compatible and interoperable with professional systems and devices the information of an organization may be accessed and distributed more easily than it used to be. If an organization does not make available to the knowledge worker the infrastructure needed to

[6] Whilst 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.

Table 8.1 Working attitudes [made by author]

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
	Private purpose	Business purpose

implement a flexible way of working, they may use their own devices and applications. Table 8.1 illustrates the differences to "traditional" ICT models at the workplace.

From an economic point of view, BYOD may seem to be an attractive solution for both, employers and employees: Whilst, employers do not need to invest in extra equipment, their employees may feel more comfortable and prove more competent and creative in handling their own devices (Drury and Absalom 2012). In fact, BYOD offers the advantages of reduced resource spending,[7] 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 creativity (ENISA 2012b: 15ff). Furthermore, it allows employees to reconcile their professional and private lives. In India, the Netherlands and the U.S., 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). The exact figure notwithstanding, it is likely that this trend will increase in Europe (ENISA 2012a; Price Waterhouse Coopers 2011: 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).

From a democratic point of view, CoIT frees knowledge workers from the limited scope of action imposed on them by the organization they work for. By using the ICT they feel comfortable with, they may fully exploit their resources and creative potential. Furthermore, perpetual cyber-access allows interested citizens to engage in democratic citizenship at all times (even at work).

However, from a security point of view, the use of consumer end-devices and applications for professional purposes hides numerous risks. While professional devices take account of security issues and are based on a server from which data is 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. Any abuse or attacks may prove detrimental to the organization concerned; Consumerized devices increase these security risks (ENISA 2012a, b). So far, most contributions to this issue have dealt with company risks (ENISA 2012a, b). However, one should also include in such an analysis

[7] 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).

Table 8.2 Advantages and disadvantages of BYOD [based on: Niehaves et al. 2012: 11]

	Advantages	Disadvantages
Employee	Autonomy Competence	Workload due to unlimited availability
Organization	Employee satisfaction Speed of adoption Employee availability Costumer focus Employee investments	Security issues Support complexity (if organization pursues a BYOD policy) Loss of process control Performance concerns

the dimension of the state and state organizations. Data thieves in the modern (hackers, skriptkids, etc.) or in the traditional sense (theft of hardware) attempting to get access to classified information might use new strategies. Business data or classified information may leak through to third or non-authorized parties deliberately or inadvertently for reasons of non-proper use by the worker (e.g. if stored on public clouds like Dropbox or if handed to third parties (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 (hacking, malware, etc. or physical attacks such as theft) (ENISA 2012a; Niehaves et al. 2012: 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 on society. 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).

Like the overall industry, states and their companies are not immune to security risks if they do not take account of CoIT. Their employees may use private end-devices and applications (e.g. store information on public clouds), if they wish to retrieve this information when not in office. Yet, as for now, national security policies have neglected the issue of BYOD. By way of example, the Austrian legislation and security strategies deal with clouds and cybersecurity, yet have neglected the issue of BYOD and are but one example of how BYOD is underestimated (Digitales Österreich 2012).

In fact, 13 of 22 chapters scrutinized by Niehaves et al. (2012: 6) revealed major weaknesses in data security. Other papers point to security risks in BYOD, too (e.g. Aerospace Industries Association 2011: 5ff). Risk mitigation is difficult—especially if the organization lacks awareness in the first place. Table 8.2 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 chapters point to employee satisfaction as the most evident advantage of BYOD and security issues as the most discussed disadvantage. Table 8.3 summarizes the risks incurred by BYOD (ENISA 2012a). Yet this analysis is based on the assumption that the state/company has implemented a BYOD policy. The x point to major effects, the (x) to side-effects.

Table 8.3 Potential risks inherent in BYOD [based on: ENISA 2012a]

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, incl. 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 (e.g. HR policies, legal scope and context and claims of ownership on intellectual property) Labour law: unofficial tele-working, 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

(continued)

Table 8.3 (continued)

Risk	Category			Explanation
	Costs	Legal	Data	
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 non-authorized 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), 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

As outlined above, general risks concern malware, economic espionage, man-in-the-middle-attacks/network-sniffing, loss of devices, etc. (Stork et al. 2012). The present state of supervisory control may not be commensurate with the vulnerabilities, threats and their potential consequences (Aerospace Industries Association 2011; ENISA 2012a). Compliance (negligence or the non-respect or non-existence 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. These variables overlap and their scope differs in accordance with the situation addressed. This is displayed in Fig. 8.2.

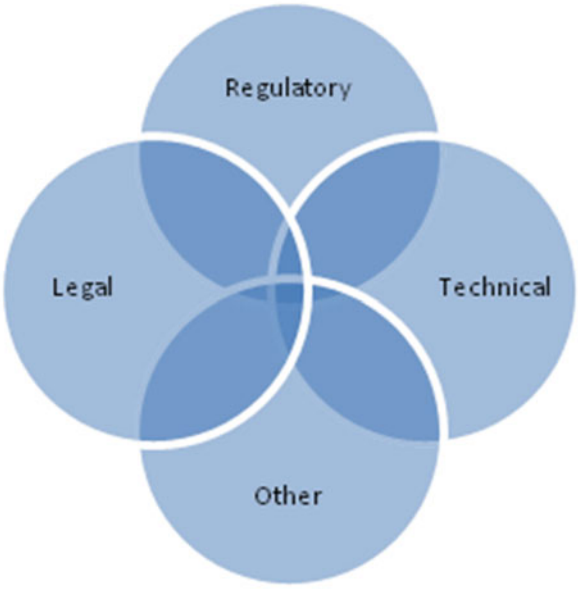

Fig. 8.2 Dimensions of BYOD management [made by author]

8.4.4 Legal Implications

The discussions about cyber-democracy, cybersecurity and cybercrime often revolve around socio-political or technical issues, often neglecting legal aspects when it comes to their implementation. Even if technical mobile device management methods may help cope with this trend, BYOD is not an entirely technical issue. Effective security management must take account of the diverse management dimensions, remain within the scope of the existing legal framework and be in harmony with the legislation in place.

According to German law, it is incumbent upon organizations to ensure data security and secrecy of telecommunications (German Telecommunications Act: Art 109; German Data Protection Act: Art 9). 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 policy. The different coping strategies are displayed in Fig. 8.3.

As it is difficult to completely restrict the use of private end-devices and applications (problem of non-respect and non-compliance), numerous papers recommend the implementation of BYOD strategies (ENISA 2012a, b). Exploring the legal implications of BYOD, the following examples shall be used: the knowledge worker holds a contract with a telecommunication service provider and uses their private

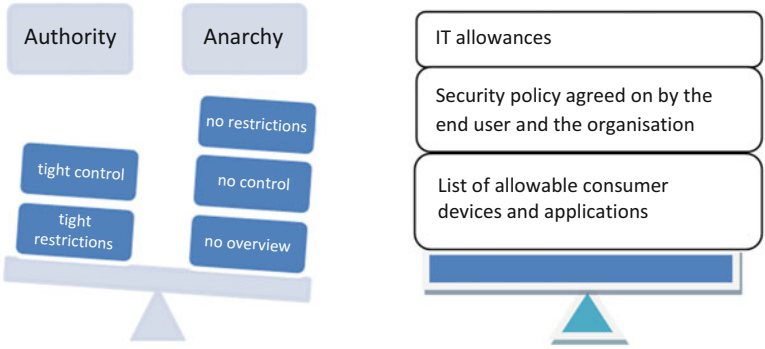

Fig. 8.3 Ways to deal with the use of private end-devices and applications in organizations [made by author]

end-device for professional purposes[8]; The knowledge worker stores professional data in public clouds (e.g. Dropbox) in order to access and process this information when out of office.

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 labour court decided that the use of non-encrypted passwords cannot entail the immediate termination of a work contract without notice if this has not been communicated beforehand (German Labour Court 2011). The employer 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 (German Labour 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 Labour Court 2009). 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 private smartphones for professional reasons seems feasible (even if unlikely), it proves extremely difficult to extend this prohibition to the whole cyberspace. 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 them (ENISA 2012c).

[8] 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.

Against this background, numerous papers recommend the implementation of a BYOD policy (ENISA 2012a, b). Awareness created through BYOD strategies helps organizations to better control this trend, even if this does not definitely rule out the non-proper handling of information, for it may never be excluded that compliance rules are disrespected.

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 (ENISA 2012b).

Moreover, it is difficult for companies to impose rules on their staff concerning the ways they use their private end-devices and different applications in their free time. Yet, in their leisure time, knowledge workers choose apps in accordance with their taste and leisure time activities. If they choose 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 2012a, b, c). 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 legislation also merits consideration. While the new paradigm of work–life flexibility dissolves the frontiers between private and professional life, labour 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. 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 difficult levels of cloud computing: IaaS, PaaS and SaaS. Yet they all have in common one basic security risk: data loss.

- 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 (ENISA 2012c)

No matter which type of cloud is being used, 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, 2012c). 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, the IT Department 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 those risks and attempt to avoid them when using their private end-devices or applications in their leisure time is likely to be much higher.

8.5 Conclusion

The emergence of the cyberspace in its present form has its origins in the Consumerization of IT. The latter has led to the democratization of IT and provided individuals with very powerful ICT. As such, it has challenged traditional approaches to knowledge creation, processing and distribution. In particular, Web 2.0 has increased the potential for democratic citizenship. The relatively new, multifaceted opportunities of the cyberspace may endorse democracy. Not only may the cyberspace 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. As such, the civil society may come to stir and participate in the decision-making processes of issues which used to be left to the heads of states and governments. The cyberspace is a strong instrument to promote global democracy and global networks and add weight to bottom-up movements. It may also further global awareness and transnational democracy.

While CoIT has paved the way for the general public to engage in cybercitizenship, it is difficult to assess if e-democracy will have a tangible effect in terms of electoral suffrage. Yet, when it comes to assessing cyber-democracy, a wide definition needs to be used, extending the typical definitions of e-democracy. Such a wide concept of democratic citizenship goes beyond electoral suffrage and includes expressions of disappointment, mistrust and disillusionment. The cyberspace has spurred their impact as it communicates them at global level.

Yet, it is difficult to draw the line between transparency, awareness-raising, civil empowerment and cybercrime, notably criminal acts of disclosure affecting businesses providing fundamental services or national security.

Since the Internet has become a fundamental service in industrialized nations, its impact on democracy and agenda-setting should definitely be observed more closely. Yet, as the cyberspaced is a decentralized space, it also spurs criminal activities. Particularly, data protection is an inherent challenge of cybersecurity.

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. Private end devices may be less secure, stolen or lost, 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 by the organization without the consent of the private owner of the device (the employee). Also, even if it is valid for the 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. Therefore, compliance is at the heart of risk mitigation strategies.

In conclusion, the cyberspace and ICT have added an e-dimension to our society. As this entails chances and challenges, a cyber-governance system is needed. This chapter presented an overview of the democratic potential of the cyberspace while pointing to the flipside of the coin, notably for businesses, but also the state when it comes to national security. Cloud solutions will not cease to be used as they prove highly efficient when it comes to the storage of large data volumes (for camera records, etc.). BYOD is a recent trend. It has not yet been assessed in terms of national security. Even if it has provoked controversy if it is worthwhile implementing BYOD strategies, all organizations—including the state—ought 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 to the organization. On the other hand, it may further their creative potential. As it is a wide field of action, it definitely needs to be evaluated in more detail. This is particularly important as ICT has become an integral part of our society.

References

Aerospace Industries Association (2011) Aerospace Industries Association (2011): Best practices for exploiting the consumerization of information technologies. Arlington, Virginia

Andriole SJ (2012) Managing technology in a 2.0 world. IT Pro(January/February), pp 50–57

Baron NS (2008) Always On: Language in an Online and Mobile World. Oxford University Press, Oxford

Barth TD (2011) The idea of a green new deal in a quintuple helix model of knowledge, know-how and innovation. Int J Soc Ecol Sustain Dev 1(2):1–14

Baskerville R (2011) Individual information systems as a research arena. Eur J Inform Syst 20:251–254, http://www.palgrave-journals.com/ejis/journal/v20/n3/pdf/ejis20118a.pdf

Benton Foundation (1998) Losing ground bit by bit: low-income communities in the information age. Benton Foundation and National Urban League, Washington, DC, http://www.eric.ed.gov/PDFS/ED424333.pdf

BITKOM (2013) Demokratie 3.0: Bedeutung des Internets für den Wahlkampf, BITKOM. http://www.bitkom.org/files/documents/BITKOM_PK_Bedeutung_des_Internets_im_Bundestagswahlkampf_07_05_2013.pdf

Brandtzaeg B, Petter B, Heim J (2009) Why people use social network sites. Online communities. Springer, Berlin, pp 143–152, http://www.academia.edu/907531/Why_People_Use_Social_Networking_Sites

Boisot M, Canals A (2003) Data, information and knowledge: have we got it right? IN 3. Internet Interdisciplinary Institute. Working Chapter Series WP04-002. 2004. http://www.uoc.edu/in3/dt/20388/20388.pdf

Campbell DFJ, Barth TD (2009) Wie können Demokratie und Demokratiequalität gemessen werden? Modelle, Demokratie-Indices und Länderbeispiele im globalen Vergleich. SWS Rundsch 49(2):209–233

Capurro R (2005) Was ist Wissensmanagement. Cogneon The Knowledge Company. http://www.cogneon.de/cp/capurro/was-ist-wissensmanagement

Carayannis EG, Barth TD, Campbell DFJ (2012) The Quintuple helix innovation model: global warming as a challenge and driver for innovation. J Innovat Entrepr 1(2). http://www.innovation-entrepreneurship.com/content/1/1/2

Carayannis EG, Campbell DFJ (2009) "Mode 3" and "Quadruple Helix": toward a 21st century fractal innovation ecosystem. Int J Technol Manage 46(3/4):201–234

Carayannis EG, Campbell DFJ (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. Int J Soc Ecol Sustain Dev 1(1):41–69, http://www.igi-global.com/bookstore/article.aspx?titleid=41959

Castells M, Cardoso G (2005) The network society. From knowledge to policy. Johns Hopkins Center for Transatlantic Relations, Washington, DC

Cavelty MD (2012) Cyber(Un)Sicherheit: Grundlagen, Trends und Herausforderungen. Polit Bild 1(2012):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. Chapter prepared for Blackwell companion to social inequalities. Blackwell Companion to Social Inequalities, Oxford

Choucri N (2000) Introduction: cyberpolitics in international relations. Int Polit Sci Rev 21(3):243–263

Schaffry A (2013) Security. Kosten und Verwaltung. Die größten Probleme bei BYOD. CIO, IDG Business Media GmbH, München

Coleman S, Blumler J (2009) The Internet and democratic citizenship: theory, practice and policy. Cambridge University Press, Cambridge

Constitution of the Federal Republic of Germany. Grundgesetz für die Bundesrepublik Deutschland. Last amendment as of 11 July 2012. Federal Gazette BGBl. I. pp 1478

D-A-CH Wissensmanagement Glossar (2010) BITKOM Arbeitskreis Knowledge Management, Gesellschaft für Wissensmanagement e.V., Plattform Wissensmanagement, Swiss Knowledge Management Forum und Wissensmanagement Forum Graz: D-A-CH Wissensmanagement Glossar. Version 1.1

Dahlgren P (2003) Reconfiguring civic culture in the new media milieu. Media and the Restyling of Politics: Consumerism, Celebrity, and Cynicism. Sage Publications, London, pp 151–170

Dell and Intel (2011) The evolving workforce: report # 1: expert insights. Round Rock, TX. http://i.dell.com/sites/content/shared-content/campaigns/en/Documents/Dell-Evolving-Workforce-Report-1-App.pdf

Digital Agenda (2010) 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

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. http://www.maximise-ict.co.uk/WP15_DiMaggioHargittai.pdf

DiMaggio P, Hargittai E, Celeste C, Shafer S (2004) Digital inequality: from unequal access to differentiated use. Social Inequality. Russel Sage Foundation. http://www.stanford.edu/group/scspi/_media/pdf/key_issues/consumption_research.pdf

Drury A, Absalom R (2012) BYOD: an emerging market trend in more ways than one. White Chapter, Ovum, Logicalis Group. http://www.logicalis.com/pdf/Logicalis%20White%20Chapter%20Ovum%282%29.pdf

ENISA (2009) Cloud computing. Benefits, risks and recommendations for information security. ENISA

ENISA (2011) Survey and analysis of security parameters in cloud SLAs across the European public sector

Clarke J, Hidalgo, MG, Lioy A, Petkovic M, Vishik C, Ward J (2012) Consumerization of IT: risk mitigation strategies. ENISA. http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/COITMitigationStategiesPublishedVersion.pdf

Clarke, Jim; Hidalgo, Marcos G.; Lioy, Antonio; Petkovic, Milan; Vishik, Claire; Ward, Jeremy: Consumerization of IT: Top Risks and Opportunities. Responding to the Evolving Threat Environment. ENISA

ENISA (2012c) 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: 9 Jan 2013. 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? Int Polit Sci Rev 27(3):221–244, Sage Publications, Ltd. http://www.jstor.org/stable/20445053

Eurostat (2013) Haushalte, die Zugang zum Internet haben, nach Art der Verbindung. http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/data/main_tables

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

Etzkowitz H (2002) The Triple Helix of University-Industry-Government Implications for Policy and Evaluation. Sister working paper, Stockholm: Science Policy Institute, November

Friedman TL (1999) The Lexus and the Olive Tree: understanding globalization. Random House, New York

German Civil Code. "Bürgerliches Gesetzbuch as of 2 Januaryr 2002. Federal Gazette BGBl. I. pp 42, 2909. Last amendment as of 7 May 2013. Federal Gazette BGBl. I. p 1122

Bundesdatenschutzgesetz (BDSG) as of 14 January 2003. Federal Gazette BGBl. I. pp 66. Last amendment as of 14 August 2009. Federal Gazette BGBl. I. pp 2814

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

Bundesrepublik Deutschland: Telekommunikationsgesetz (TKG) as of 22 June 2004. Federal Gazette BGBl. I. pp 1190. Last amendment as of 3 May 2012. Federal Gazette BGBl. I. pp 958–1717

Betriebsverfassungsgesetz (BetrVG) as of 25 September 2001. Federal Gazette BGBl. I. pp 2518. Last amendment as of 20 April 2013. Federal Gazette BGBl. I. pp 868. geändert worden ist

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. 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

Harris JG, Ives B, Junglas I (2011) The genie is out of the bottle: managing the infiltration of consumer IT into the workforce. Accenture Institute for High Performance. http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Managing-the-infiltration-of-Consumer-IT-into-the-workforce.pdf

Hammond AL (2001) Digitally empowered development. Council of Foreign Relations: Foreign Affairs

Halavias A (2009) Search Engine Society. Polity, Cambridge

Infosecurity Magazine (2012) Crystal ball time: top 2013 risks include cyber war, cloud and BYOD. http://www.infosecurity-magazine.com/view/29570/crystal-ball-time-top-2013-risks-include-cyber-war-cloud-and-byod

International Standards Organisation ISO/IEC 27005 (2011)

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. http://www.computerworlduk.com/in-depth/mobile-wireless/3349518/byo--ive-hidden-costs-to-a-bring-your-own-device-progamme/

Kettinger WJ, Li Y (2010) The infological equation extended: towards conceptual clarity in the relationship between data, information and knowledge. Eur J Inform Syst 19:409–421

Klein A, Vöhringer B, Krcmar H (1999) Cyberdemocracy – Neue Chance für Demokratie? http://www.winfobase.de/lehrstuhl/publikat.nsf/intern01/076790EF7CDE06A84125686C002CCFCD/$FILE/99-19.pdf

Leigh D, Harding L (2011) WikiLeaks: inside Julian Assange's war on secrecy. The Guardian

Leiner BM, Cerf VG, Clark DD, Kahn RE, Kleinrock L, Lynch DC, Postel J, Roberts LG, Wolff S (1997) A brief history of the Internet. Internet Society. http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Leiner

Lennon RG (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

Lewitzki M (2011) Das Internet in Parteiform: Wie segelt die Piratenpartei? Student Chapter. Regierungsforschung.de. NRW School of Governance. Universität Duisburg Essen. http://regierungsforschung.de/data/070111_regierungsforschung.de_lewitzki_piraten.pdf

Livingstone S, Ólafsson K, Staksrud E (2011) Social networking, age and privacy. EU Kids Online, London, UK. http://eprints.lse.ac.uk/35849/1/Social%20networking%2C%20age%20and%20privacy%20%28LSERO.pdf

Loader BD, Mercea D (2011) Introduction networking democracy Social media innovations and participatory politics. Inform Commun Soc 14(6):757–769

Martinez E, Rajlkashmi S (2012) Workplace 2030. People matters. http://www.peoplematters.in/articles/focus-areas-13/what-is-hot/workplace-2030

Maier R, Thahmann S, Bayer F, Krüger M, Nitz H, Sandow A (2008) Flexible office: assignment of office space to enhance knowledge work productivity. J Univ Comp Sci 14(4):508–525

Mitterlehner B (2013) Daseinsvorsorge als europäischer Begriff. In: Der europäische Antagonismus – Binnenmarkt und Daseinsvorsorge. Schriftenreihe Daseinsvorsorge Band 1. Public Social Responsibility Institut

Mitterlehner B, Barth TD (2013) Daseinsvorsorge: Grundaufgabe und Begriff. In: Der europäische Antagonismus – Binnenmarkt und Daseinsvorsorge. Schriftenreihe Daseinsvorsorge Band 1. Public Social Responsibility Institut

Moore G (2011) Systems of engagement and the future of enterprise iT—a sea change in enterprise IT. AIIM, Silver Spring, MD

Moschella D, Neal D, Opperman P, Taylor J (2004) The "Consumerization" of information technology. CSC, El Segundo, CA, http://www.smaele.nl/edocs/Taylor-Consumerization-2004.pdf

Murdoch R, Harris JG, Devore G (2010) Can enterprise IT survive the meteor of consumer technology? Accenture Institute for High Performance. 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: Becker J et al (eds) Working chapters. European Research Center for Information Systems No. 13. Münster. http://www.ercis.uni-muenster.de/sites/default/files/publications/2012/ercis_working_report_13_-_consumerization_0.pdf

Nowotny H., Gibbons M., Scott P (2003) *'Mode 2' Revisited: The New Production of Knowledge*. In Minerva 41:179–194

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. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Olsen RK (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. IEEE Comput 44(9)

Papacharissi Z (2010) A private sphere: democracy in a digital age, polity. Cambridge

Price Waterhouse Coopers (2011) The consumerization of IT – the next generation CIO. Center for Technology and Innovation, New York

Poster M (1995) CyberDemocracy: Internet and the public sphere. University of California, Irvine, CA, http://www.hnet.uci.edu/mposter/writings/democ.html

Rettberg JW (2008) Blogging. Polity Press, Cambridge

Rose C (2013) BYOD: an examination of bring your own device in business. Rev Business Inform Syst Sec Quart 17(2). The Clute Institute. http://www.journals.cluteonline.com/index.php/RBIS/article/view/7846/7906

Sambharya RB, Kumaraswamy A, Banerjee S (2005) Information technologies and the future of the multinational enterprise. J Int Manage 11(2):143–161

Squires J (1998) In different voices: deliberative democracy and aestheticist politics. The politics of postmodernity. Cambridge University Press, Cambridge, pp 126–146

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 Jul 2012

Treaty on the Functioning of the European Union (2008) C 115/50

Chapter 9
"Creating" a Public Sphere in Cyberspace: The Case of the EU

Johanna Diecker and Matthias Galan

Abstract Information and communication technologies (ICT) are seen as a potential cure to democratic deficits within the political framework of the European Union (EU). They are regarded as a means to overcome the inherent legitimation deficit. This article discusses the potential for democratic innovation through ICT-based solutions within the EU-framework and their role in the emergence of a European cyber public sphere. Against the background of deliberative theory of democracy, two European cyber-democracy projects are analysed and compared to scrutinize their democratic merit: the Open Consultation and the European Citizens' Initiative (ECI). The authors come to the conclusion that these initiatives are successful to some extent, yet stay behind their possibilities.

Keywords Democratic legitimacy • Democratic innovation • Deliberative theory • European Union • ICT-based communication • Online consultation • European Citizens' Initiative • Cyber-democracy

9.1 Introduction

In an increasingly globalised world, patterns of the relation between citizens and the government are more and more underlying significant changes. Globalisation is questioning the model of the Westphalian state and produces a context in which the scope of social organisation does no longer necessarily reflect its territorial boundaries.

J. Diecker (✉) • M. Galan
Freelance Researcher, Vienna, Austria
e-mail: johanna.diecker@gmx.de; matthias.galan@gmail.com

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_9,

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, is a prime example for this process (Eriksen 2009:8).

Related to discussions on the transformation of the state are continuing public as well as academic discussions on democratic legitimacy. *One position* is asserting the erosion of the normative quality of democratic government. From this point of view, 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 supranational 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. 2007:2).

Due to the continued success of information and communication technologies (ICT), they are more and more seen as a potential cure to the many issues related to democratic governance and its 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" (Carrara 2012:356). Furthermore, these 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" (ibid.). As civil society organisations (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 (ibid.). Therefore the EU's engagement of 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 (ibid.).

For this reason we would like to engage the complex of EU cyber-democracy by assessing implications and the possible benefits of participatory elements in the EU decision-making process. We will discuss the potential for democratic innovation and the emergence of a European cyber public sphere, which we consider as precondition for EU cyber-democracy.

This analysis will scrutinize participatory instruments within the EU framework based on a deliberative approach to democratic theory and assess their potential for democratic innovation subsequently to the model introduced by Graham Smith (see Smith 2009). *First*, we will outline theoretical framework of deliberative democracy and the cyberspace. In a *second* step, we will discuss current implications of a European public sphere and the normative turn towards participation of European citizens in decision-making processes. We will continue with an analysis of two strongly ICT based participatory instruments: online consultations and the European Citizens' Initiative. Finally, we will compare the two instruments and assess the innovative momentum through ICT, based on the model of democratic innovation by Graham Smith.

9.2 Deliberative Democracy and the Cyberspace

The changes in political behaviour we encounter nowadays, give proof to the fact that democratic legitimation is more than just voting. It is "rather the normal actions of citizens, as citizens, voting, lobbying, doing none of these things if they choose, protesting, organizing and as subjects, obeying rather than avoiding the law, and making rather than avoiding their contributions, particularly in the form of taxation, to public expenses" (Barker 2007:32).

At the moment there are two dominant perceptions of legitimacy: One of these perceptions is the differentiation in input legitimacy, defined as participation in democratic procedures, and output legitimacy, comprising problem solving and control over the incumbents of power. The second perception is based on the relationship of popular sovereignty and human rights. Drawing on the work of Habermas, human rights are perceived as the fundament for democracy here. This universalistic approach addresses the prerequisites of democratic systems on a global or supranational scale (Hurrelmann et al. 2007:4).

If we follow the discussions focusing on input legitimacy, the mobilisation of citizens becomes a crucial issue for political institutions. Paradoxically, the participation of such engaged citizens has for a long time been considered as a danger to thriving democracies. "Mainstream" democratic theory, as in the works of Schumpeter or Dahl, considers democracy rather as a way of choosing political elites than as a way to guarantee the direct rule of the people. Therefore, and in the light of mass movements in the first half of the twentieth century, participation as a way to secure democratic legitimacy was for a long time neglected (Monaghan 2012: 288).

With the emergence of deliberative approaches to democracy promoted by the works of Jürgen Habermas, this mind set started to change. Instead of emphasizing a rather formalistic approach of parliamentarian deliberation, the procedural medium of a discursive decision-making process is highlighted. In order to adapt democracy to the results of social and institutional change, democratic processes need to be reconsidered (Schmalz-Bruns 2009:76).

The basic idea that Habermas expresses, is that the comparison of existing democratic procedures to a procedural blue print would allow the development of an internal relation between pragmatic considerations, compromises and discourses, which can under the precondition of problem-oriented information flows and a suitable treatment of information lead to reasonable and fair results. The normative argument would therefore be based on communication and communicative socialisation (Habermas 1998:359 ff.).

To assess the quality of such deliberation a public sphere, as a discursive arena, is crucial. It is here where people can discuss questions of public interest. The public is separated from the state and market and is reflecting the livelihoods of the participants. In an ideal case this arena would enable free, unrestricted and rational communication. In a "perfect" public sphere individuals are able to control the actions of political as well as private actors. The underlying concept can be understood as a blue print for assessing legitimacy and efficiency of public opinion (Fraser 2009:148).

In the terminology of Jürgen Habermas the public sphere is a network to exchange opinions, in which communication flows are concentrated into public opinions. The environment of the public sphere reproduces itself through communicative action, where a "natural" language is sufficient to understand a discourse (Habermas 1998:436). At the same time the public sphere constitutes a very complex network, which has different, sometimes overlapping arenas. These are structured by thematical emphasis, policy area and other view points, which are nevertheless understandable for ordinary people. The public sphere, defined through the relation to the political system, therefore stays permeable (ibid.:452).

This concept of a public sphere allows for the analysis of societal and European integration as it makes it possible to conceptualize the emergence of such a public sphere as the result of European communication networks. A major precondition in such a concept is that a common political culture carried by civil society (interest groups, NGOs, citizen initiatives and movements) is put into existence or is already in place. It is civil society actors who have to "conquer" arenas in which political parties reflect on decisions by the European institutions and accelerate the creation of European parties (Habermas 1997:184).

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 following the rules of the discourse, legitimacy is created. By drawing on discursive rules rather than normative presumptions on power relations, deliberative democracy is setting itself apart from expert or elite oriented approaches. 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 organised and acceptable to its constituents. Communicative power has to be understood as societal power which is based on communication as an open and collective formation of opinion. Only under these circumstances is a democratic public sphere possible (Möllers 2009:259 ff.).

Ongoing technological innovations and the increased differentiation as well as interconnectedness of modern societies are a precondition to allow deliberative democracy and are promising a further strengthening of democratic legitimacy. With seemingly endless possibilities of evolving technologies to make use of freedom of speech, opportunities to exchange, challenge opinions, and to spread ones views, mobilisation and participation might seem easy to be realised. However, 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 (Kies 2010:3). Other authors rather think that participants engaging in these debates are already politically active, which would all in all not increase participation. As computer mediated communication is rather "based on anonymity, absence of direct contact, and absence of moderation", some scholars also doubt "the emergence of qualitative and accountable political debates" (ibid.).

Related to the question of the actual increase of participation through online deliberation, there are normative questions as well as technical challenges with implications for democratic legitimacy. Legitimacy has always to be considered as

being highly influenced by power relations and the dynamics within a given framework, which is in this context the cyberspace. According to Rogg, three points are of importance in this regard. *Firstly* we have to consider transparency, as 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 actually able to consider this information. *Thirdly*, there is a certain selectivity regarding information made visible through new technologies and other information, which is not reported at all (Rogg 2003: 77/78).

This raises the question on the relation between cyberspace and the public sphere and especially how it can be conceptualised. It is an ongoing process with very diverse and dynamic communication networks. Nevertheless, 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 rather "centripetal" forces (Dahlgren 2005:152).

The mixed system of ICT enhanced democracy we see nowadays—especially if we do consider the case of the EU—is likely to lay the ground for a central prerequisite of cyber-democracy, being a diversified and equal cyber public sphere. Cyber-democracy has to be seen as another sphere transferring democratic legitimacy that is depending on and interrelated with other democratic practices as well as based on technical requirements.

9.3 The Case of the European Union

The European Union, as one of the major examples for new globalised 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 2009:2). 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 organisations, what status has it acquired? The definition debate has produced many different possibilities to describe the EU—transnational organisation, 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 multidimensional policy network" (Karr 2006:90).

9.3.1 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 2009:5). 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 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 2012:17).

In order to help us analyze the democratic deficit of the EU and the opportunities the evolving cyber-democracy brings, we can heuristically distinguish European democracy in institutional terms into *a polity* where authorised 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 2012:19). 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 though our analysis 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 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 whilst the council is often criticised 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 supranational and transnational construct. Democratic legitimacy is always grounded on the collective will formed by 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. 2012:169). This paradox is inherent for processes of democratisation. 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. 2012:173).

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 globalisation and new means of communication "polymorphus, polyphonic, and even anarchistic" (Eriksen 2009:123). But in order to analyze the impact of changing means of communication on the public sphere, the term public sphere needs further operationalisation. 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 (institutionalised discourse among persons legally authorised to make collectively binding decisions) (Eriksen 2009:130).

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 audiovisual 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 organised in the national context and European topics play only a secondary role (Karr 2006:99ff; Eriksen 2009: 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 Organisations (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 2006:128).

Still these segmented publics and CSO as one of their main actors, are seen as transmission belts 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 shaped through political means and civicness as a tool for the construction of identity (Eriksen 2009:73; Freise 2008:26 f.; Friedrich 2008:71). 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" (v. Finn 2008:59). Especially Eastern European CSO lack capacity and face therefore difficulties in placing their issues on the EU agenda (ibid. 2008:55 f.).

9.3.2 From Partnership to Participation: The EU's Normative Turn

Deliberative democracy offers alternative legitimisation paths to democratize the EU beyond representational democracy given the weak input legitimacy of the EU due to the institutional set-up—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. 2012:298). 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: 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 realisation of participation on a practical level (Dalakiouridou and Smith 2009:5).

Regarding secondary legislation, "until 2000, the predominant view of democracy was implicitly connected to public access to documents (…)"(Dalakiouridou and Smith 2009:5). 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 2001:10) and gives thus 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" (Haibdbreder 2012:15). The most important follow-up tool was the Interactive Policy Making platform that got the focal point for online consultation at EU level (Dalakiouridou and Smith 2009:5).

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. 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. 2012:308). 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. 308ff; 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 2009:6). The website "your voice in Europe"[1] 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 not mentioned on this page is the ECI, which is the youngest initiative for online participation on the EU level. Our analysis will scrutinize both, the online consultation and the ECI in terms of democratisation and increased legitimacy.

9.4 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 would be a cyber-public sphere capable of allowing for stronger involvement of citizens in democratic procedures.

[1] http://ec.europa.eu/yourvoice/index_en.htm

The model, which we would like to apply 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 2009:11). In this analytical framework the emphasis is put on four democratic goods, "namely inclusiveness, popular control, considered judgement and transparency" (Smith 2009:12). These four goods are indispensable to an understanding of democratic legitimacy, even if the way in which each of those goods is emphasised in single theoretical approaches might be differing. 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 2009:13).

This "matrix" allows us 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 operationalisation 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 2009:21). 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". Therefore it is crucial to assess inclusiveness and the degree to which it has been realised (Smith 2009:22).

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 judgement focuses 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, it is also related 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 too as publicity, describing the "transmission of information about the institution and its decisions to the wider public" (Smith 2009:25). The strategies organisers 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 in the media (Smith 2009:26).

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 2009:26).

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.).

9.5 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 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. Whilst 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 at any place. However, if a closer look is taken at the realities of the different member states, it becomes clear that there is still 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 % (Seybert 2012:1 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 today for online participation. Especially Eastern European countries are very likely to be 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 these tools can have in this imperfect environment for democratic legitimisation.

9.5.1 The European Commission's Online Consultation Tool

Online Consultations (OC) 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 is so far the main mean of citizen involvement, though it might be challenged by the ECI in the near future, with sometimes more than 100 OCs taking place per year. However, their use varies widely across Directorate Generals (DGs). Furthermore they are a voluntary tool of the EC (Quittkat 2011:658 ff.; Dalakiouridou et. al. 2012: 316).

Upon the announcements of OC on the web portal, different target groups can give their opinions. In the "open" target group all range of actors and interested parties are welcome to participate. Selective OC generally address well defined groups on rather technical issues whilst closed OC are limited to business and business organisations, public authorities, or both. The format of a consultation process ranges from standardised (closed questionnaire), to semi-standardised (questionnaire with open questions) and non-standardised (text can be freely commented). Consultation is open for a minimum of 2 months and after evaluation the EC should publicly report on the inputs and their evaluation. OC can take generally place at any stage of policy making. However, it tends to be used the most in the initial phase of the legislative cycle (Quittkat 2011:653, 660 ff.).

The OC is expected to increase the democratic legitimation of the EU. Being in place for over a decade now, empirical and scientific data on the results has been collected and evaluated (see Quittkat 2011). Against the backdrop of the operationalisation of deliberation by Smith, we will scrutinize whether the OC has lead 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.

9.5.1.1 Inclusiveness

New channels like the OC generally lead to an increased access of organisations and interest groups to EU institutions and decision making processes. 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 %), providing at least formal access and inclusion for all interested groups to the vast majority of OC (Quittkat 2011:660; Haidbreder 2012: 16; Karr 2006:128).

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 2011:667). Often business and business-associations make up 39 % of all participants in an 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, business seem 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, and due to the necessary amount of expertise and resources to effectively participate in an OC, it is only highly professionalised and Brussels-based interest groups WHO remain the standard representatives of CSO. "Until now, the pre-existing 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 2012:16). 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 a critical and independent CSO arena (Friedrich 2008:78).

9.5.1.2 Popular Control

"For the time being, the participation of civil society organisation has to be characterized as 'participation by grace and favor'" (Friedrich 2008:78). OC are no exception as they are only implemented on a voluntary basis, depending on the will of

individual civil servants. Therefore their impact differs widely across the different DGs, policy fields and levels (Haidbreder 2012:16). Moreover, about two thirds of OC are used 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 that seeks input from experts rather than offers actual decision making authority (Dalakiouridou and Smith 2009:3; Haidbreder 2012:16). "The more concrete the facts of a case, the less the Commission is prone to consult the wider public" (Quittkat 2011:660).

The format restricts real popular control over decision-making as many of the OC are using the semi-standardised or standardised 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 (2011:662).

Overall, the OC has 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.

9.5.1.3 Transparency

The OC has increased transparency to a certain degree, as it gives online access to information and allows interest groups to potentially influence 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 2012:16). Especially the reporting part on consultations 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 2011:664).

Regarding transparency, especially the use of modern communication technologies would put the 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.

9.5.1.4 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 contributors do

have an understanding of technical details. However, other positions in the "debate" are not disclosed and therefore not 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 was given to their concerns (2008:78 ff.).

To facilitate considered judgment, transparency would be a prerequisite. To design consultation more in a form of a 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, as they fail to meet requirements of one of the main characteristics of deliberation.

9.5.1.5 Efficiency and Transferability

The adoption of OC lowers the cost of information dissemination and feedback collection. Especially standardised 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 to different policy fields and also EU institutions. The Council or the Parliament could theoretically adopt OC and simply use the software of the EC.

9.5.1.6 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—a process 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 through the initiative of the EC. 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 Brussels-based associations only. "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" (Haidberder 2012:26). 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 2009:150).

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 plethoras 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 2009:150), even if only to a limited extent as in the case of the OC.

9.5.2 The European Citizen Initiative

The European Citizens' Initiative (ECI) was already included in the Treaty establishing a Constitution for Europe "during the Convention on the Future of Europe (2002–2003) as part of a broader article whose aim was to introduce participatory democracy in the EU (art. 47)" (Garcia and Del Rio Viller 2012:312). It allows EU citizens to invite the EC to propose an amendment or new piece of legislation to the European Parliament (EP) and Council. In an early stage it was foreseen to become a key driver for public debates. This trigger function for a more sustainable debate on different issues concerning the EU and its institutions was at the start emphasised (Monaghan 2012:292). 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, which is required in some member states to verify a signature (Monaghan 2012:294).

CSO have already used ECIs before their formal introduction through the regulation 211/2011. As Carrara explains these ten ECIs already were to a big extent relying on the Internet to collect support and share information (Carrara 2012:356). 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.:366). Also the preamble to regulation 211/2011 establishing the ECI highlights the importance of modern information technologies to offer the necessary framework for the citizens' initiative in paragraph 14 (EC 2011).

There are several general requirements that have to be matched by organisers and by signatories. *First* of all, the ECI can only be organised and endorsed by European citizens, who are allowed to vote in elections to the European Parliament (Szeligowska and Mincheva 2012:276). *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.: 277/278). *Thirdly*, it has to meet formal requirements such as information on the initiative and its purpose (ibid.: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 need to have met a minimum threshold of signatures, "which is established by multiplying the number of MEPs [Member of European Parliament] of the Member States concerned by a factor of 750". An initiative needs to collect

this minimum requirement in 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.).

According to Greenwood, these requirements create a lot of administrative and technical costs for the organisers (Greenwood 2012:330). For the first initiatives this can be confirmed, as they already have had many technical problems, which was acknowledged by the EC in a statement in 2012 saying that it was necessary to "throw a lifeline to organisers of the first European citizens' initiatives (ECIs) by exceptionally offering to host their online signature collection systems on its [the EC's] own servers" (EC 2012). In addition the 12 months timeframe for the collection of the required statements of support was extended, because organisers were not able to find suitable host providers on the market for collecting signatures online (ibid.). There was a strong reaction of 75 MEPs to these shortcomings at the end of February 2013, as they sent 6 parliamentary questions on issues with the ECI to the EC. This included issues such as serious technical and administrative problems that are delaying the process and creating high costs and the flaws of the open source software for online signature collection provided by the EC. This software is considered to be too complicated to handle and full of mistakes that cannot be properly reported to the commission (EP 2013a). Furthermore, estimates are that 11 million EU citizens who live outside their home country are denied their right to support ECIs (ibid.). In April 2013 the commission answered to the concerns raised by MEPs denying that there have been bigger problems and confirming its cooperation with organizers (EP 2013b). According to the official registration website of the EC, there are 16 initiatives open for collection of statements of support. Nine initiatives have been so far refused registration and 5 have been declared obsolete.[2] We will now turn to an analysis on the potential for democratic innovation of the ECI and ICT as a crucial factor for participation in the ECI.

9.5.2.1 Inclusiveness

The regulation 211/2011 establishing the ECI, aims to include all European citizens who are allowed to vote in EP elections. This is already a selection mechanism, as people not holding a European citizenship but being residents within the European Union, are excluded. One of the central aspects of inclusiveness is access, on the one hand to relevant information on the issues, which the ECI wants to solve and on the other hand to the process itself. This requires for both organisers and supporters a significant amount of ICT literacy and access to the Internet (EC 2011).

As Garcia and Del Rio Villar argue, the ECI is another mechanism that might be used to contribute to the policy-making process by enabling citizens and their organisations to "introduce legislative proposals" (Garcia and Del Río Villar 2012:316).

[2] European Commission: European Citizens' Initiative—Official register. http://ec.europa.eu/citizens-initiative/public/initiatives/ongoing

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 claim that current participation is elitist and constituted by already organised lobbying groups and organisations, which use the ECI to gain influence (Monaghan 2012:290). Language and ICT-knowledge are also a relevant selection mechanism for citizens, who want to participate in an ECI. They have to be able to speak English as this is widely used as lingua franca and to use the Internet (Carrara 2012:356).

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 organisers and the verifying Member States need to make sure that signatories are real persons and their signatures can be counted as genuine (Carrara 2012:363). Regarding the collection process of statements of support, there are controversies because of differing requirements demanded by Member States as some use ID numbers to verify signatures and others do not (Monaghan 2012:294).

The ECI can be seen as an important step in the direction of a stronger inclusion of European citizens in European decision-making processes. It might be a bit too early to comment on its overall innovative momentum for inclusion, but potentially it allows for a wider discussion of EU policies led by CSO which provide for the necessary resources and information. Furthermore, it enables citizens to better understand that there are in fact common concerns which can be raised on the European level.

9.5.2.2 Transparency

Transparency is to a certain extent assured by publishing relevant documents and information on EU websites, which is a minimum standard (Smith 2009:25). There is support for citizens and organisers who either want to get information or start a new ECI. Therefore conditions for participation are to a certain degree transparent. Still there needs to be overall improvement regarding the availability of support to organisers and participants as well as a clearer picture on what happens after an ECI was successful, for instance when it comes to drafting legislation.

9.5.2.3 Popular Control

The ECI as a participatory tool is meant to enable public control over the shaping of policies. According to article 4 paragraph 2 and 3 of the regulation establishing the ECI, the Commission is obliged to carefully examine every registration and if rejected has to give a statement on the reasons 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 2012:315).

Nevertheless, the question if there should be a deeper accountability of the EC and the institutions is not yet solved. Recently, one of the citizens committees asked the European Court of Justice to review the rejection of the ECI "One million signatures for a Europe of solidarity" by the EC. The forthcoming court ruling might give a better idea of possibilities to hold the EC accountable through the judicial system of the European Union (The ECI Initiative 2013a).

Overall popular control is quite weak as it is only in the first two of the four stages of decision-making, problem definition and option analysis, where citizens can take control. 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 2012:316). If compared to other popular referendums the ECI therefore might have less impact on decision-making processes. Furthermore, the non-binding nature of the ECI leaves its political significance to the willingness of the Commission and the legislative bodies to decide on the political demands by the citizens (Cuesta-López 2012:267). Nevertheless, the possibility for citizens to "formally participate in the EU decision-making process" by presenting their initiative to the institutions can be considered "a significant evolution for the EU political system" (Garcia and Del Río Villar 2012:319).

9.5.2.4 Considered Judgement

As evidence from the ECI shows, enabling citizens to come to a considered judgement is a challenging task not only for the institutions but also for organisers. A significant part of dissemination of information about the ECI is done through "websites and social media/networks such as Facebook, Twitter, etc" (Carrara 2012:358). Already in this information stage of piloting ECIs most organisers did avoid to open multilingual online forums as costs would have been too high. This fact reiterates that language as well as Internet literacy are crucial for considered judgement and in the context of the EU very challenging in practical terms (ibid.:357). There are further limitations in developing online strategies. When the ECI enters the phase of convincing people and collecting signatures "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.:358). This shows that linguistic resources are crucial to allow citizens to come to a considered judgement. Language therefore is still a "strong limitation to citizens' discussion and deliberation in the process of ECIs" (ibid.357).

One remedy to this problem would be a truly pan-European media landscape to enable citizens to get information on political issues (Carrara 2012:356). So far examples, e.g. Euronews have shown that these remain limited to the 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 2012:267). 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 2012:320). 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.).

9.5.2.5 Efficiency

At this point of time it is hard to tell if ECIs will be able to really offer a citizen friendly instrument, enabling a stronger connection between citizens and institutions and therefore strengthen input legitimacy. Efficiency of procedures is crucial for future success. Recent developments and issues with registration and online tools 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 regulations or directives based on an ECI. Regarding the costs and benefits there are not only material considerations 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 2012:318). 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 2012:296).

9.5.2.6 Transferability

Similar and related to efficiency, transferability will be depending on the successful implementation of the ECI (Monaghan 2012:296). What we can observe already is that ICT and online tools do have to stand up to minimum standards allowing citizens to easily understand and act in accordance with given regulations. If the tools right now in use are further developed, they might be a benefit to other levels of governance.

9.5.2.7 Way Towards a European Public Sphere and Cyber-Democracy

In relation to other participatory instruments within the EU framework, e.g. the civil dialogue, success of ECI supporters in reaching their objective might be rather small. This being said, it depends on the EC and other EU Institutions to take the outcome of ECIs seriously (Garcia and Del Río Villar 2012:318). 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 organisers, while one million signatures might be easy to dismiss in comparison to the overall EU population (ibid.:319).

The ECI certainly increases discussions on topics related to the EU, but the question still remains, who will be willing and able to mobilise a wider public to rally for a common cause. Initiatives since the early 2000s have shown there is quite a lot of failure to "mobilise a wider public" by civil society organisations, 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 2012:307). Therefore a closer examination of problems with the mobilisation of the public for EU policy issues would be necessary (ibid.).

9.5.3 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 organised 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. However, barriers that prevail in the analogue world, like language barriers, are also prevailing in a 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 resembled 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 raises inclusiveness and equality to an extent never seen before in the EU though critics fear that it is already being hijacked by the Brussels 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 does not meet the requirements of transparency to a sufficient extent. The ECI is at least designed to fulfil these minimum requirements during the process. However, what happens after a successful ECI is rather intransparent as further steps are left to the EC and the legislative institutions EP and Council.

Whilst the OC is clearly not designed to put decision-making authority into the hands of CSO, the ECI gives at least public control over first steps of the policy cycle. Though both initiatives are non-binding, the ECI can put through public discussion more pressure on the EC. However, if and to what extent an ECI will have a real impact on decision-making remains to be seen in the future.

The OC does 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 judgement 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 struggles with a missing European media landscape. A stronger promotion of the ECI itself might be a starting point. Potential for considered judgement therefore is given in its design and will probably evolve further in the future.

Both initiatives are transferable and basically also efficient though they request a high resource input resulting in the distortion of participation in favour of organised 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 could draw on made experiences and was introduced a decade later. 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 the EC.

All in all—have web-based forms of participation led to the development of a European public sphere? The initiatives are addressing different layers. While the OC remains in the sphere 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 professionalised 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 2011:672).

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 is 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 2012:292). 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. 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.: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.).

Recent sociological work shows that elites in the EU are indeed merging into a stronger interconnected community, leaving most of the citizens behind. So far, deliberative procedures do not have a "rapid, ground-shaking, substantive impact" (Haibdbreder 2012:25). 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 mobilise a wider public. However, the ECI gives the citizens an active part in the communication by giving them a voice. If and how this will eventually lead to the emergence of a European public sphere is depending on other types of media and to what extent European citizens will make use of the tool.

In conclusion we can say 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. 2012:318). While the OC clearly fails, the ECI might possess this ability.

9.6 Conclusion

The ICT revolution is just at a starting point and likewise democratic practices based on ICT will need time to gain acceptance as sources of democratic legitimacy. As for now the outlook might be rather that conventional democratic practices in combination with ICT 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. 2012:177).

Our analysis shows that EU institutions should further pursue a positive attitude towards ICT and democratic legitimacy. But 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, both with their big potential and shortcomings, by developing such coherent strategies based on a strong commitment to participation. First of all it will be necessary to assess where it makes sense to promote ICT in democratic procedures at the European level and develop long-term sustainable solutions.

If the EU fails to properly address and stand up for the development of direct democratic online tools this might lead to serious disappointment and even bigger loss of legitimacy, driving citizens away from ICT-based solutions. As trust is one of the key elements of democratic legitimacy it will be necessary to develop reliable tools, which are user-friendly and at the same time meet security and privacy needs and rights of EU citizens.

References

Barker R (2007) Democratic legitimation: what is it, who wants it, and why? In: Hurrelmann A, Schneider S, Steffek J (eds) Legitimacy in an age of global politics. Palgrave MacMillan, New York, NY, pp S.19–S.34

Carrara S (2012) Towards e-ECIs? European participation by online Pan-European mobilization. Perspect Eur Polit Soc 13(3):352–369

Cuesta-López V (2012) A comparative approach to the regulation on the European Citizens' initiative. Perspect Eur Polit Soc 13(3):257–269

Dahlgren P (2005) The Internet, public spheres, and political communication: dispersion and deliberation. Polit Comm 22(2):147–162

Dalakiouridou E, Smith S, Tambouris E, Tarabanis K (2012) Electronic participation policies and initiatives in the European Union institutions. Soc Sci Comput Rev 30(291):297–323

Dalakiouridou E, Smith S (2009) Contextualising public (e)participation in the Governance of the EU. Eur J ePractice 7. http://www.epractice.eu/files/ePractice-Journal-Volume-7.pdf]. Accessed 22 July 2013

De Clerck-Sachsse J (2012) Civil Society and democracy in the EU: the Paradox of the European Citizens' initiative. Perspect Eur Polit Soc 13(3):299–311

The ECI Campaign (2013): European Court of Justice to Rule on Admissibility of an ECI for the first time. Released on 19 July 2013. http://www.citizens-initiative.eu/?p=1832. Accessed 23 July 2013

The ECI Campaign (2013): 75 MEPs ask EU Commission to urgently improve the European Citizens' Initiative. Released on: 4 April 2013. http://www.citizens-initiative.eu/?p=1578. Accessed 23 July 2013

Eriksen EO (2009) The unfinished democratization of Europe. Oxford University Press, Oxford

Eriksen EO, Fossum JE (2012) Europe's challenge. Reconstituting Europe or reconfiguring democracy? In: Eriksen EO, Fossum JE (eds) Rethinking democracy and the European Union. Routledge, London, pp 14–38

European Commission (2013): Press release of Commissioner Michel Barnier Statement by Commissioner Michel BARNIER on the exclusion of water from the Concessions Directive. Released on 21 June 2013. http://ec.europa.eu/commission_2010-2014/barnier/docs/speeches/20130621_water-out-of-concessions-directive_en.pdf. Accessed 24 July 2013

European Commission (2012) Commission offers own servers to help get first European citizens' initiatives off the ground. (press statement). http://ec.europa.eu/commission_2010-2014/sefcovic/headlines/press-releases/2012/07/2012_07_18_eci_en.htm. Accessed 24 July 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 June 2013

European Commission (2001) European Governance. A white paper. http://eur-lex.europa.eu/LexUriServ/site/en/com/2001/com2001_0428en01.pdf. Accessed 22 July 2013

European Parliament (2013a): Parliamentary questions—26 March 2013, Subject: one year of European Citizens' initiative (ECI) in practice: evaluating experience and tackling obstacles. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+OQ+O-2013-000033+0+DOC+XML+V0//EN. Accessed 23 July 2013

European Parliament (2013b) Parliamentary questions—10 April 2013, E-001851/2013 answer given by Mr Šefčovič on behalf of the commission. http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2013-001851&language=DE. Accessed 23 July 2013

v. Finn H (2008) Assessing Civil Society in Europe: comparative findings of the CIVICUS Civil Society Index. In: Freise M (ed) European Civil Society on the road to success? Nomos, Baden-Baden, pp 45–63

Fraser N (2009) 2. Theorie der Öffentlichkeit. In: Brunkhorst H (Hg., 2009) 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: Freise M (ed) European Civil Society on the road to success? Nomos, Baden-Baden, pp 23–43

Friedrich D (2008) Actual and potential contributions of Civil Society organisations to democratic EU-Governance. In: Freise M (ed) European Civil Society on the road to success? Baden-Baden, Nomos, pp 67–86

Garcia LB, Del Río Villar S (2012) The ECI as a democratic innovation: analysing its ability to promote inclusion, empowerment and responsiveness in European Civil Society. Perspect Eur Polit Soc 13(3):312–324

Góra M, Mach Z, Trens H (2012) Situating the demos of a European democracy. In: Erik EO, Fossum JE (eds) Rethinking democracy and the European Union. Routledge, London, pp 159–178

Greenwood J (2012) The European Citizens’ Initiative and EU Civil Society organisations. Perspect Eur Polit Soc 13(3):325–336

Habermas J (1998) [1992]: Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats. Suhrkamp, Frankfurt/Main

Habermas J (1997) Die Einbeziehung des Anderen: Studien zur politischen Theorie. Suhrkamp, Frankfurt am Main

Haidbreder EG (2012) Civil Society participation in EU Governance. In: Living Reviews in European Governance, vol 7, No. 2. http://europeangovernance.livingreviews.org/Articles/lreg-2012-2/download/lreg-2012-2Color.pdf. Accessed 22 July 2013

Hurrelmann A, Schneider S, Steffek J (2007) Legitimacy in an age of global politics. Palgrave MacMillan, Basingstoke

Karr K (2006) Democracy and lobbying in the European Union. Campus Verlag, Frankfurt

Kies R (2010) Promises and limits of Web-deliberation. Palgrave Macmillan, Basingstoke

Möllers C (2009) 13. Demokratie und Recht. In: Brunkhorst H (Hg.) Habermas-Handbuch. Metzler, Stuttgart [u.a.], p S.254–S.263

Monaghan E (2012) Assessing participation and democracy in the EU: the case of the European Citizens‘initiative. Perspect Eur Polit Soc 13(3):285–298

Quittkat C (2011) The European Commission’s online consultations: a success story? J Common Market Stud 49(3):653–674

Rogg A (2003) Demokratie und Internet: der Einfluss von computervermittelter Kommunikation auf Macht, Repräsentation, Legitimation und Öffentlichkeit. Verlag Leske + Butrich, Opladen

Schmalz-Bruns R (2009) 15. Demokratie. In: Brunkhorst H (Hg.) Habermas-Handbuch. Metzler, Stuttgart [u.a.], p 75–81

Szeligowska D, Mincheva E (2012) The European Citizens’ initiative—empowering European citizens within the institutional triangle: a political and legal analysis. Perspect Eur Polit Soc 13(3):270–284

Smith G (2009) Democratic innovations: designing institutions for citizen participation. Cambridge University Press, Cambridge

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

Part III
Cyber-Defense

Marios Panagiotis Efthymiopoulos

The policy on Cyber-Defense is the most important collective policy that is currently conducted and developed. It aims to counter both current and new, symmetrical and asymmetrical threats locally but also globally. In the framework of national security of each state, major organizations and major companies seek to develop a Cyber-Defense protection from any possible threats. Cyber-Defense is due to emerge as the most important security challenge in the first 20 years of the twenty-first century. Cyber-Security is referred for the protection of a variety of installations: from a simple computer and Internet connection and mobile telephones to national or private major infrastructures, such as water and electricity supplies. In the twenty-first century, the world is more e-interconnected than ever. As such there is an increasing need to adopt new methods and actions for cyber-protection against existing threats and possible challenges to emerge in the future. This section will be looking for new technical and political methods and actions, to counter ever-enlarging challenges and threats in a 21st cyber-world. In addition to Cyber-Defense this section aims to explore the relations of Cyber-Defense with democracy and development in an era of global fiscal crisis when effective technological tools limit human capital and increase technological knowledge, innovation, and production. In war, future war-like operations 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. Military and Police missions, will continue to require agile and networked, well-trained, and well-led forces. This section will contemplate themes of Cyber-Defense and Security, as well as emerging theories and values, legal aspects, transatlantic links (NATO, international organizations, and bilateral relations between states, and global trends and attempts otherwise stated as global challenges in a net-centric worldview context).

Chapter 10
Cyberspace as a State's Element of Power

Nikitas Nikitakos and Panos Mavropoulos

Abstract Cyberspace is becoming increasingly central to states' economies and their societies. This growing role of cyberspace has opened up new opportunities but at the same time created new threats, which states have to live with, finding ways to identify and mitigate them. Cyberthreats are created by the exploitation of vulnerabilities inherent in every manmade system to include cyberspace, by various actors which are usually grouped in four categories, namely, organized criminals, hactivists, foreign governments and terrorist groups. The last two actors are closely related to national security, in its narrow sense; they use cyber power against (other).

Keywords Cyberspace • Cyber power • Cyberwar • Cyber deterrence • (Distributed) denial of service (DDoS) attack • Elements of power • DIME • Critical infrastructure

10.1 Introduction

Cyberspace, as much as it is difficult to define, is a reality, having intruded in our lives gradually, reaching today a point without return; no one can live without it anymore. Although cyberspace exists since the invention of electromagnetic transmission, in its contemporary perception came into existence with the appearance of

N. Nikitakos
University of the Aegean, Chios, Greece
e-mail: nnik@aegean.gr

P. Mavropoulos (✉)
Hellenic Army Academy, Athens, Greece
e-mail: pmavropoulos@yahoo.gr

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_10,

personal computers (circa 1975), the Internet protocol (circa 1982) and the World Wide Web (circa 1989).[1] Today, a continuously increasing portion of the international human activity is being conducted within or through this expanding notional space. Governments have become increasingly dependent on cyberspace; businesses around the world tender services and products through the Internet to more than 2.5 billion citizens using secure protocols and electronic payments. Services range from e-government, e-banking, e-health and e-learning to next generation power grids, air traffic control and other essential services, all of which depend on the cyber infrastructure. In some countries the Internet, as the major component of cyberspace, contributes up to 8 % of gross domestic product.[2]

Lacking an overarching regulatory authority, cyberspace's operation is chaotic resulting in serious issues that need to be dealt with by the states, as the most important actors of the international system. The chaotic operation of cyberspace provides the opportunity to various actors, i.e. hackers, crackers, criminal gangs, terrorist groups, hacktivists, states or even groups of states (standing or ad hoc alliances), to resort to illegal activities (Denial of Service [DoS] attacks, Distributed Denial of Service [DDoS] attacks, Web defacements, infecting systems with malware), each one with its own aims and objectives ranging from personal data stealing up to infecting major state critical infrastructures with malware. Illegal activities in cyberspace constitute a serious threat for the general security of a nation-state, including its narrowly defined national security.

States, very well aware of the existing threats for their security, have long ago initiated actions for protecting their cyberspaces, by preventing, deterring, defending against and recovering cyberattacks. In doing so, they are seeking to strike a balance between stimulating their economy and improving national security, infrastructure modernization and critical infrastructure protection, private sector and public sector, data protection and information sharing, freedom of expression and political stability, which NATO handbook refers to as five dilemmas.[3]

"The economic, technological, political and social benefits of cyberspace are at risk if it is not secure, protected and available. Therefore, the availability, integrity and resilience of this core infrastructure have emerged as national priorities for all nation-states."[4] For the protection of their cyberspace, states take a multilevel approach by building a comprehensive cyber security strategy for a safe, secure and resilient cyber environment.

[1] Caton, *What do senior leaders need to know about cyberspace*?

[2] Hathaway and Klimburg, *Preliminary considerations*: *on national cyber security*, p.1.

[3] Luiijf and Healey, *Organizational structures and considerations*, p.120.

[4] Hathaway and Klimburg, *op. cit*., p.3.

10.2 Concepts and Definitions

The term *cyber* is both ambiguous and controversial. The lack of a widely accepted definition of *cyber* terms in general and *cyberspace* in particular is thought to be a major drawback. On the other hand, it is rather premature to hope for a consistent and detailed definition of cyberspace to be adopted by all parties involved in cyber business. As long as this human endeavor evolves, analysts prefer to use the respective terms in descriptive texts, at least until accepted definitions are introduced. As a result, the existing definitions of the term *cyberspace* present considerable differences in the way different states and/or different international organizations view it. The descriptive definitions found in the international literature range from a narrow understanding which describes it as coincided more or less with the Internet (Australia, Canada, Germany, New Zealand, Spain, etc.) through a broad view which is thought to include infrastructures (the USA, Holland, etc.).[5] It seems though that the international actors realize the ever expanding and changing nature of the new medium and therefore the respective definitions are both changing in time and are expressed in a flexible way in order to adapt accordingly and accommodate new developments, as required. Despite those problems, and for the purpose of this chapter, we will define the terms *cyberspace* and *cyberwar*, albeit in a descriptive form.

Most of the people define cyberspace as the space which includes the infrastructure accessible via Internet. In general, cyberspace is not just the Internet, although it is the most known, prominent and larger part of it, and is not restricted to "all the world's computer networks".[6] Should we restrict cyberspace to the Internet, we definitely exclude a large part of what is called cyberwar, which deals with isolated systems. Those systems, which require an air-gap between themselves and the rest of the world, are thus not exposed to the outside electromagnetic environment; they are accessible through other means, the global maintenance supply chain being the most important one. The only way to affect those systems, apart from their physical destruction, is to infect them with malware in the form of logic bombs, programmed chips and planned in sensitive material, which are triggered when certain conditions are met.[7] We would like to think of cyberspace as the space which is not restricted to the Internet, but includes also isolated networks, all industrial systems connected to the Internet or to isolated networks through Supervisory Control And Data Acquisition (SCADA) systems, the communication and information systems industries, as well as spare parts and software production industries, all academic institutions related to the information technology in general, and people and social interaction within the above.[8]

---

[5] Lindstrom and Luiijf, *Political aims & policy methods*, p.56.

[6] Krepinevich, *Cyber warfare*: *a* "*nuclear option*"? p.8.

[7] In 1982, an explosion tore apart a natural gas pipeline in Siberia. The planning and execution of the operation has been attributed to the CIA. Clark and Levin, *Securing the information highway*: *how to enhance the United States*' Electronic Defenses and Libicki, 2009, *Cyberdeterrence and cyberwar*, p.21.

[8] Hathaway and Klimburg, *op. cit*., p.8.

If the term *cyberspace* is ambiguous, the same applies to the war waged in cyberspace, namely, cyberwar, for which there is no official or generally accepted definition. War, in its traditional perception, can be defined as the threat of use or the actual use of military power, aiming at imposing one's own will onto that of its potential enemy. Through the course of human history though, international actors used other means as well, short of military power, to change the target political entity's behavior, i.e. diplomacy, economy, psychological means and more recently cyber power. Reserving the term *war* for the armed conflict, we usually refer to this form of imposing our will on the enemy as war, with a respective prefix which characterizes the particular means used, i.e. diplomatic war, economic war, psychological war, information war, electronic warfare, with the most recent addition that of cyberwar. Therefore, *cyberwar* is a state of conflict between political entities resorting to cyberattacks in pursue of their political aims. Cyberwar can be combined with any other form of war, or it can be waged as a standalone activity. Despite the difficulties with the term *cyberwar*, it is used widely in current public discourse. It is only natural though for polemics of the term to exist, one of which argues that "'cyberwar' …is not…just a meaningless neologism, but strategically a distracting and nonsensical one. Contemporary strategists who reckon that 'cyberwar' is a decisive new form of conflict are wrong"[9] and calls for the prefixed war types, which shift that focus onto technology itself, to be rejected. Despite the objections, others consider that the term has a useful academic purpose, because "it concentrates thinking on state to state conflict" and "has become an unavoidable element in any discussion of international security".[10]

Having explained what we mean by the terms cyberspace and cyberwar, we now proceed to examine the actors resorting to illegal activities in cyberspace and what sort of threat they pose for a state.

10.3 Actors and Threats in Cyberspace

Cyberspace is becoming increasingly central to states' economy and theirs societies. The growing role of cyberspace has opened up new opportunities but at the same time created new threats, which states have to live with, finding ways to identify and mitigate them.

The actors in cyberspace are usually grouped in four categories,[11] namely, organized criminals, hactivists, foreign governments and terrorist groups.

Criminals are involved in all sorts of illegal activities, such as credit card details and other personal data theft, which are used for gaining economic benefits.

[9] Betz, *Cyber war is not coming*, p.21.

[10] Hathaway and Klimburg, *op. cit*., p.17.

[11] This typology is adhered to by a considerable number of countries in their national cyber security strategies. For a typical example see relevant documents by the UK and New Zealand.

Politically motivated activist groups (hactivists) or ideologically motivated individuals seek to gain control over computer systems or websites and use them to promote their particular cause, make a political statement or disrupt services, and thus gain publicity.

In peacetime, foreign governments, through their military and intelligence services conduct cyber espionage against government systems, national infrastructure and businesses seeking access to commercially sensitive information, intellectual property and state or trade secrets. Cyber espionage against governments was given serious consideration when sensitive information started being stored on networks. It reached its peak in this cyber era. Numerous incidents are reported each year with progressively increased seriousness,[12] in which governments and private companies experience significant losses of intellectual property. The new cyber capabilities not only made the old job of espionage easier, safer and enormously more efficient, but they attained their own life, being able to pursue goals in a totally different way. In crises or even armed conflicts, foreign governments can (and will) use cyberspace to inflict harm on critical systems in support of their wider aims.

Foreign governments, in pursue of their goals in cyber space, may request cyber services from proxies in the form of "patriotic" hackers or even mercenaries[13] in the form of individual lone hackers, groups or criminals and pay for those services.

There is a strong rational for which terrorist groups would resort to cyber power in order to inflict harm, pain and terror onto their intended target states and their societies; cyber weapons are cheap, easy to acquire or even to develop; cyberattacks do not require the perpetrators' physical presence in the target-states and can be launched from almost any point of the globe; terrorists' most preferred target-states (western) present a target rich environment and progressively expose high-value targets to possible cyberattacks; "fire and forget" tactics and anonymity fits perfectly to the modus operandi of those groups; retaliation is practically not possible. Despite all aforementioned advantages, terrorists seem so far reluctant to use cyberspace as a priority battle field, because "it is doubtful that they would generate the level of widespread panic and terror"[14] they desire.

For the purpose of this chapter, we would like to distinguish hactivists and organized criminals, whose activities fall within the authority of law enforcement agencies, even though those are related to security in the general sense of the word, from foreign governments and terrorist groups, which resort to cyber activities for pure political reasons against primarily a rival state's national security.

Those actors by the nature of their activity in and through cyberspace create an evolving cyberthreat environment. Cyberthreats thus created are continuously

[12] For an updated list of cyber incidents, including cyber espionage ones, visit www.csis.org (significant cyber events).

[13] Humanity has not seen mercenaries since the dark ages; today, their use should not be ruled out, albeit in different form.

[14] Liff, *Cyberwar*: *A new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war*, p.423.

increasing and evolving in sophistication and frequency. Understanding those threats is of paramount importance for the protection of cyberspace by security professionals.[15]

Today, no state is immune from cyberattacks. Governments and private companies' systems have been under attack through cyberspace for many years now. A well-planned cyberattack can disrupt public services, interfere with the production and delivery of essential goods and services impacting negatively upon the economy or resulting in the theft of intellectual property or personal information and, ultimately, threatening national security.

Cyberthreat deserves and in fact attracted states' attention as a new and evolving threat which has become a major security concern of political and military leaders around the world.[16] Security in world politics though is neither a neutral, nor a simple idea[17] and its perception varies among politicians and scientists alike. The difficulty and perplexity of the issue is best depicted in the fact that different scientists express different perspectives vis-à-vis security. Many of those argue that the traditional view of security (what Booth calls "Trinitarian[18] view of security"[19]) is typically associated with the realist's view of International Relations and is focused on the traditional meaning of the term: the military security of nation-states which puts the state at the center.[20] A number of scientists argue that this view of security is a legacy from the Cold War, when the referent was the sovereignty of the state and its territorial integrity, while the only element of power of the state primarily suitable for this kind of threat was the military.[21,22]

This view of security has been contested in recent decades and relatively recently has been moved away from the Cold War traditional definition of security as narrow military. New national security issues came into the fore and the concept has been broadened and deepened to include these nontraditional threats. This new approach to security, though still not very well defined, is addressed by many scientists; Castles and Miller argue that the contemporary security environment comprises of the net result of many security indicators, such as national, economic, health and social.[23]

---

[15] Marinos and Sfakianakis, *ENISA threat landscape*: *responding to the evolving threat environment*.

[16] Liff, *op. cit*.

[17] Booth, *Critical security studies and world politics*.

[18] The characterization of security as "trinitarian" stems from the Clausewitz's view of war as a "paradoxical trinity" (Clausewitz, *On war*, p.89), which today is used to characterize wars amongst nation-states or wars of the industrial age.

[19] Booth, *op. cit*.

[20] Nadig, *Human smuggling*, *national security*, *and refugee protection*; Castels and Miller, *The age of migration*.

[21] Though we are generally in agreement, we would extend this state-centric approach to include the period from the Peace of Westphalia, when the modern nation-state started emerged firstly in Europe and then elsewhere.

[22] Nadig, *op. cit*.

[23] Castels and Miller, *op. cit*.

This relatively new kind of security is threatened by all sorts of threats, with cyberthreat being one of the recent and major ones. For the rest of the chapter we will focus on cyberthreats posed by actors in cyberspace against nation-states. As noted above, the majority of those come from foreign governments and their proxies, as well as terrorist groups.

There are certain characteristics of cyber power, account for its growing popularity, which makes it attractive to various actors resorting to illegal activities in cyberspace for their own purposes. Those characteristics are unique and therefore the means and ways to fight them should be tailored to theme, should we like to stand any chance of success:

- Cyberattacks in cyberspace are inexpensive in the sense that respective malware can easily be acquired for a modest price or even downloaded for free from the Internet.
- Resources needed to launch an attack are limited, to their lower end, to computers or smart phones and malware which can be easily acquired. At the same time, actors with basic skills, with help from numerous sites in the Internet can cause considerable damage.
- Cyberattacks can be launched from far away and geographically dispersed origins, contributing thus to difficulties in the detection and already problematic prosecution of perpetrators.
- Perpetrators of illegal activities run a low risk of detection and prosecution, being able to hide their tracks.

10.4 The Purpose of Cyberwar

As it applies to the overarching concept of war in general, cyberwar (and any war in that sense) is not an end in itself but it is rather conducted for the purpose of achieving political ends. Those political ends, decided by the political leadership of the entities engaged, can be seen from many different points of view. The ultimate purpose of any war though is to impose one's own will onto that of his opponent.[24]

Submission to the opponent's will is obviously decided by the respective government, following a cost-benefit analysis and taking into account many factors. One of these factors is the will of the people. Therefore, planning our strategy against an opponent, one of the options is to erode the will of the opponent's people, which in its turn can be done in many different ways. The North Vietnamese tried it successfully during the Vietnam War by resorting to a protracted war, which finally eroded the American people's will to support the case.[25] This strategy is not new at all though. Italian Air Force Major General Giulio Douhet, the first air power theorist,

[24] Clausewitz, *On war*.

[25] Summers, *On strategy*: *a critical analysis of the Vietnam War*.

in his book published in 1921,[26] highlighted the moral effects of aerial attacks which could "…be directed…against objectives of least moral resistance",[27] referencing "peacetime industrial and commercial establishments; important buildings, private and public; transportation arteries and centers; and certain designated areas of civilian population as well"[28] as targets. Attacking those targets one can inflict fear among the civilian population and ultimately erode its will to support the war. Along the same argument, Nagasaki and Hiroshima were not any high value military targets to be attacked with atomic bombs. They were picked for destruction in order to attack the will of the Japanese government and people to continue the war and not the capabilities of the Japanese military forces.

Danny Steed argues that cyber power cannot coerce as kinetic force does.[29] That may be so, but while coercion is obviously not the strong point of cyber power for the time being, cyber capabilities continue evolving. It will not be long before cyber power will be able to cause large scale harm and destruction, even as a second order effect. Today though, cyber power has the potential to be used as a means to inflict pain and fear onto the opponent's people and erode its will to the point where it will exert pressure to its government for submission to the aggressor's will.

While there is truth in Danny Steed's statement that "[t]here has simply not been enough experience of actors utilizing Cyber means to attain political ends…",[30] and in Martin Libicki's similar one that "[t]here are reasons to doubt that cyber war has what it takes to coerce a state. No one has yet died in a cyber attack",[31] 2 years after Steed's paper and 4 years after Libicki's book the cyberworld looks very different; there is already enough evidence that cyber power has reached at a maturity stage to be used credibly enough for the attainment of political ends; they might not be glorious as those attained through military power, but at least they fit to its particular characteristics.

In conclusion, cyber power's attainable aims is the undermining of the opponent's people will, by inflicting pain and fear amongst them, which in turn can be done by attacking the respective state's critical capabilities.

10.5 Strategy in the Age of Cyberspace

When cyber power presented serious evidence as a new and "important domain in interstate conflict"[32] theorists and strategists started work about possible approaches to prevent or defend against cyberattacks or even attack within or through cyberspace

[26] Douhet, *The command of the air*.

[27] *Ibid*., p.22.

[28] *Ibid*., p.20.

[29] Steed, *Cyber power and strategy*: *so what*?

[30] *Ibid*., p.23.

[31] Libicki, *op.cit*., p.124.

[32] Goodman, *Cyber deterrence*: *tougher in theory than in practice*? p.103.

against other states. Seen from this point of view, "cyber power has posed a challenge for strategists since its advent, and the questions have only grown more pressing with the revelation of the Stuxnet malware attacks on Iranian nuclear sites".[33]

The development of cyber capabilities by governments, being those powerful computers or sophisticated pieces of software created a new and important domain of power.[34] The development of this type of power is not an exclusive privilege of states, but it is shared with a wide variety of actors that coexist in cyberspace. This "diffusion of power in cyberspace will coexist and greatly complicate what it means to be a sovereign state or a powerful country".[35]

Cyber power thus acquired is currently used by various actors to conduct any sort of illegal activities in cyberspace. We have previously distinguished cyber activities in two broad categories; those that fall under the authority of the law enforcement agencies and those that belong to the realm of narrow defined national security, with the latter being our focus in this chapter. We should be careful though with the use of the term *cyberwar* to characterize activities in cyberspace, even when the actors are nation-states. So far "state-to-state computer network attacks there have not been; espionage, yes, of course; irritating hacktivism, certainly; but cyber war, no, at least not by a careful definition".[36] Most of these activities in cyberspace today are about cyber espionage and economic benefits, which even if discovered are not revealed, because this will harm the reputation of the victim and will reveal its vulnerabilities to the rest of the world.

With the aforementioned caveat in mind, we argue that there is no cyberwar without a political aim decided by a respective political entity, a term which could include individual states, groups of states (standing or ad hoc alliances), supranational organizations, revolutionary movements and terrorist groups. All these actors, depending on their capabilities and will can initiate and sustain cyberwar against one or more of the other actors in the list; activities of other actors in cyberspace, i.e. lone hackers and criminals, cannot be characterized as war by any criterion.

There are many interesting issues associated with the conduct of cyberwar, which all belong to the tactical–technical level. Public discourse almost ignored discussion of cyber power beyond this level; tactical–technical level cyber talk dominated international literature (and in fact still does) since the appearance of the term *cyber*. With the exception of very few papers, the use of cyber power to achieve political ends, which is the realm of strategy, has been the object of books and articles only recently or to put it in Colin Gray's words; "High-quality strategic theory about cyber simply is not there in the literature during the 1990s and most of the 2000s".[37]

This is not the essence of cyberwar though; what matters the most is the purpose of using cyber power against other state or non-state actors. Cyberwar is not an end

[33] Milevski, *A special operation in cyberspace*, p.64.

[34] Gray, *Making strategic sense of cyber power: why the sky is not falling?* Nye, *Cyber power*.

[35] Nye, *op. cit*., p.2.

[36] Gray, op. cit., p.4.

[37] *Ibid*., p.7.

in itself; it is conducted in pursue of a wide variety reasons, which in strategic theory parlance are called *political ends*. Otherwise, the illegal activity within cyberspace is called crime and falls inevitably within the realm of law enforcement agencies. The real issue though we need to ask ourselves and, ultimately, answer, is the purpose for which we should raise and use cyber power, in other words, what is the political aim cyber power will be used for. Because, no matter how good we become in executing cyberwar, it is all irrelevant if we have not chosen a clear-cut political end to be pursued, suited to the particular characteristics of cyber power, a notion expressed two centuries ago, albeit for military power, by the great Prussian General, theorist and philosopher of war, Carl von Clausewitz, in his monumental work *On War*.

Almost all strategists and cyber power experts alike tend to equate cyber power with military power or, even worst, to consider it as subordinate to military power.[38] This in its turn means that cyber power, when considered in the context of a crisis or actual war, should play a supporting role to that of military operations. That may be so in some, rather limited, cases but this consideration underestimates cyber power, its dynamics and prospects. Cyber power differs from military one in the sense that it cannot kill directly and cannot occupy territories[39]; but the same applies to the other state's elements of power, namely, diplomacy, economy and information. If war is seen as an effort to impose one's own will on that of the enemy,[40] then cyber power can be considered as a means to that end (with other means being diplomacy, information, military, economy (DIME)), an autonomous element of power, with its own special characteristics and capabilities.

Cyber power, following a slow start in a supporting role to the other elements of power, took its own life and reached today a point where it can seek to achieve, as a primary element of power, political ends, with the other elements of power in supporting roles. As cyberspace expands quickly to include progressively larger portions of human activity and at the same time cyber capabilities evolve, those political ends will expand to include more ambitious ones.

Lacking the essential elements of causing harm and damage, as argued by the majority of experts, for coercing potential enemies, the question raised is how an actor, using its cyber power, can influence the political behavior of a potential enemy. In other words, where cyberattacks should be directed, what the cyber objective would be and what the center of gravity of the potential enemy would be for the cyberwar effort to be directed against.

The strategic objective of a general cyberattack, in the context of a cyberwar aiming at influencing a potential opponent's political behavior, is the will of the opponent state's people.[41] The target of the cyberwar should be the people and indirectly,

[38] Martin Libicki argues that "The establishment of the 24th Air Force and US Cyber Command marks the ascent of cyberspace as a military domain. As such, it joins the historic domains of land, sea, air, and space." Libicki, 2009, *op. cit*.

[39] Steed, *op. cit*.; Libicki, 2009, *op. cit*.

[40] Clausewitz, o*p*, *cit*.

[41] Miller and Kuehl consider "social cohesion and political will" as one of the multiple objectives that cyberattacks will likely have (Miller and Kuehl, *op. cit*., p.2).

the government, which is ultimately responsible to make the final decision of possible yielding to the opponent's will. The will of the people can be attacked by creating chaos in the country and undermining the confidence of the people in its government vis-à-vis its capability to provide basic services to them. This in turn can be achieved by attacking the potential opponent's information technology infrastructure. The standardization of components required in the information technology industry, which is done primarily for economical reasons, exposes those systems to cyberthreats. No system with information technology infrastructure is excluded, no matter if it is connected to the Internet or not.

An important subset of the information technology infrastructure is a state's critical infrastructure, which is defined as the infrastructure vital to its functioning and providing basic services to its citizens. Generally, the critical infrastructure includes electricity production and distribution systems, communication networks and services, economic institutions, transportation, food production, etc. "At the heart of many of these critical infrastructures is an Industrial Control System (ICS) that monitors processes and controls the flow of information. Its functionality is like the on or off feature of a light switch. For example, an ICS can adjust the flow of natural gas to a power generation facility, or the flow of electricity from the grid to a home. Over the last decade, industry has increased connections to and between critical infrastructures and their control system networks to reduce costs and increase efficiency of systems, sometimes at the expense of resiliency".[42]

Attacks on critical infrastructures have been going on for years now, aiming (for the moment) not at their destruction. Nearly two-thirds of critical infrastructure companies report regularly finding malware designed to sabotage their systems.[43] According to the British National Cyber Security document[44] the attacks are implemented in four different ways, namely, electronic attack, subversion of supply chain, manipulation of radio spectrum, disruption of unprotected electronics using high power radio frequency, which means that no electronic system is immune to cyberattacks.

One of the most preferred critical infrastructures for cyberattacks is the power production and distribution system of a potential opponent. Preparation for this kind of attacks has already begun many years ago. In January 2008 a CIA official said the agency knew of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply for four foreign cities. In February of 2013 the US Department of Homeland Security issued a restricted report, revealing that from December 2011 through June 2012, cyber criminals targeted 23 gas pipeline companies and stole information that could be used for sabotage purposes.[45]

---

[42] Hathaway and Klimburg, *op. cit*., p.7.

[43] McAfee, *Critical infrastructure protection report*, March 2011.

[44] UK Cabinet Office, *The UK cyber security strategy*: *protecting and promoting the UK in a digital world.*

[45] www.csis.org, Significant cyber events.

A state's critical infrastructure will be a priority target on which the enemy's cyberattacks will be directed, provided they are, in some way, accessible. Organized cyberattacks against critical infrastructures can not only cause substantial economic costs on the intended target country, but they can also cause chaos in the functioning of the target state, while at the same time can cause, even indirectly, harm and damages, bringing everyday life almost to a halt, undermining the people's will and its confidence to its government.

Most states, realizing the importance of critical infrastructure and the need to be protected from external attacks maintain a list of their critical infrastructures, along with their vulnerabilities and the means for their protection.

If war is the realm of politics and political leadership, and warfare is the realm of military and its leadership, then in whose realm does cyberwar fall? Cyberwar, due to its particular nature, is a means at the disposal of a nation-state's government or a non-state actor to manage a crisis and therefore can be characterized as one of the elements of power of a state, in addition to diplomacy, information, military power and economy. In this context, the use of cyberpower for the attainment of political ends is planned at the grand strategy level, in other words at the political level.

10.6 Cyber Warfare: The Conduct of Cyberwar

Anonymity is a buzz word for cyberspace specialists, not unfounded though; it is a "function of the identity-obscuring architecture of cyber space"[46]; along with its associated concept of non-attribution, which is rather problematic, it is one of the most referenced characteristics, responsible for the reputation cyber power enjoys today. A careful consideration of this characteristic though reveals that it is not always useful and desirable. In peacetime, the activities in cyberspace, seen from the national security point of view, are limited to cyber espionage, training and preparations for future possible crises and actual conflicts by infecting possible enemy states' critical capabilities and relevant military targets. In this case anonymity is a major advantage and prerequisite for successful cyber operations. In crises and actual conflicts though, hiding the attacker's identity is meaningless. Betz is right; "[O]ne's enemy needs to know whose thumb they are under so that he may be surrender, or render 'cash payment' in return, as Clausewitz put it".[47]

In some cases though, when cyberattacks are launched against a state, the attacker might want to keep his identity obscured, while at the same time wants the victim to know who he is. In this case, he needs to strike a balance; on the one hand he wants the victim to know who the perpetrator is, retaining at the same time the "non-attribution" advantage. That was the case of cyberattack against Estonia in 2007, when everybody assumed that the perpetrators were the Russians, while Russia never assumed responsibility for the attacks. In these cases, cyberwar and anonymity is an oxymoron.

[46] Betz, *op. cit*., p.22.

[47] *Ibid*., p.23.

States, before resorting to war, including cyberwar, are suppose to try and exhaust any available mean to resolve the issue. Even in the case of failure of every other option, states should, and usually will, try to deter potential cyber aggressors. One of the first issues examined in recent years in the context of the potentiality of using cyber power was that of deterrence and if it can be applied in cyberspace. Almost all analysts agree with Martin Libicki's conclusion that "cyber deterrence is highly problematic",[48] or Joseph Nye's similar one that "[d]eterrence is limited and difficult because of problems of attribution of the source of an attack".[49] On the other hand, there is no one who denies that defense is absolutely necessary in trying to avoid serious troubles in cyberspace. While this is true, pursuing political ends through the use of cyber power is not possible without offensive capabilities, which is why state and non-state actors acquire cyber power. Offense is the strong point of cyberwar; it is easy, not expensive, maintains the initiative etc.; or to put it in Colin Gray's words; "Cyberspace is by its scientific nature an environment friendly to offense, rather than defense".[50]

One of the most advertised characteristics of cyberspace is that it is "borderless". The question raised in this case is how this affects the use of cyber power by the international actors in the context of a cyber conflict. The implication of this characteristic on the way cyberwar is conducted is important, but only when it is compared to the way kinetic war is conducted. The reason for the association of the two is due to the fact that cyberwar, once initiated, has a high probability to escalate in a kinetic war.

Let us consider a cyberwar between two states that they cannot escalate to kinetic war, which applies when they do not share borders and lack power projection capabilities that reach their opponent. It is obvious that the political ends sought through cyberwar are limited mainly because of its particular characteristics and therefore such a cyberwar cannot be characterized as total, in the sense that Ludendorff, in his famous book,[51] attributes to the term "total". In this case, cyberwar is a restricted one. Of course, it can escalate to an unrestricted cyberwar in relation to the means employed; both cyber belligerents will employ every available cyber capability to achieve the purpose.

If no one seems to achieve the purpose and depending on the issue being at stake, cyberwar can escalate to a kinetic war. This escalation presupposes that one or both cyber belligerents possess respective capabilities. In this case, cyber power, in order to be effective, has to be combined with the threat of use of physical force. This combination does not undermine the importance of cyber power as an independent element of power; the same applies to the other elements of power; neither diplomacy nor economy can achieve decisive results unless supported by a credible threat of use of kinetic force. The threat of use of kinetic force and escalation to traditional war is certainly and undoubtedly applied for belligerents that share borders, irrespective of their international power status, namely, if they are superpowers, strong powers or even small states.

[48] Libicki, 2009, *op. cit.*, p.176.

[49] Nye, *op. cit.*, p.5.

[50] Gray, *op. cit.*, p.41.

[51] Ludendorff, *Total war*.

For belligerents that are geographically located far apart, the threat to use kinetic force and the likely escalation to kinetic war is possible for the actor(s) who possesses power projection capabilities that reach the opponent. If only one possesses such capabilities, then we fall in the classical case of asymmetry between the belligerents. Asymmetry, as it is meant in this work, is the considerable difference in power (cyber and/or military/kinetic), strategy or tactics between actors. One of the experts on power, Joseph Nye, underlines that "[t]he characteristics of cyberspace reduce some of the power differentials among actors, and thus provide a good example of the diffusion of power that typifies global politics in this century".[52] David Betz, on the other hand, argues that "[f]ar from demonstrating a smoothing of the existing asymmetry of power amongst states it actually shows a reinforcement of that asymmetry: cyber power rewards already powerful states".[53] Though in the international literature it is implied that the use of cyber power by a weak state or non-state actor against a stronger state constitutes asymmetry, this is important because combined with anonymity and non-attribution, makes the life of the stronger power hard in combating such phenomena. Resort to traditional war seems inevitable.

In the case that both cyber belligerents possess kinetic force capabilities that can be used against the other, escalation to traditional war will depend on a number of factors, including the importance of the national interest at stake.

In the case that both belligerents lack such capabilities, cyberwar is destined to end, even if no-one from the belligerents yields. This brings forward an interesting point. Cyber power makes easy for the political leadership the decision to resort to cyberwar against another state, when he cannot physically attack the first, especially when "[t]he idea that cyber power could be a war-winner, or, at least, the key player on the national security team, is by no means absurd. Indeed, it is prudent for defense analysts today to explore and examine the net strategic promise in cyber power to see how great its strategic benefits and dangers might be".[54]

10.7 Cyber Power vs. Military Power

As mentioned before, cyber power, being one of the state's elements of power, cannot be subordinated to military power. This is not to say that the military should ignore cyber power. On the contrary, with military's increasing dependence on cyberspace, there is an absolute requirement for defending its own systems exposed to the enemy's cyberattacks, while at the same time developing suitable capabilities for undermining the enemy's hard power by attacking its systems within and through cyberspace (Quite naturally the same applies to the other elements of power as well). Cyberspace though is something that reaches beyond military power. Its relation to military power

[52] Nye, *op. cit.,* p.19.

[53] Betz, *op. cit*., p.23.

[54] Gray, *op. cit*., p.34–35.

is the same as with the other elements of power, namely, supporting-supported relation. In other words, depending on the state of affairs we are at, there is one primary element of power with the rest in supporting roles; this relationship changes as the state of affairs develops from peace to crisis and possibly into war.

Many analysts, despite the impressive improvement of cyber capabilities in the last two decades, still prefer to see cyber power as "a real and important compliment to other military capabilities"[55] or highlighting its inability to "neither harm individuals nor destroy equipment (albeit with some exceptions)" conclude that "cyber war can only be a support function for other elements of warfare, for instance, in disarming the enemy".[56] Martin Libicki goes on to make a projection in the future that cyber power "…is likely to remain so indefinitely".[57]

This support function is materialized as cyberattacks against military targets and military related civilian targets. In an interesting article back in 2009, Robert Miller and Daniel Kuehl reserved a particular role for cyberattacks in relation to kinetic war; that of the "first battle" or "opening shot" of the war (which sometimes is called electronic Pearl Harbor). In their article, they explained that "the first battle in any future conflict…will be electronic and waged in/via cyberspace". Those cyberattacks will be directed against "enemy communications and supply lines", enemy "command and control" systems, "enemy infrastructures", enemy's "social cohesion and political will", "to shape global perceptions of the conflict", while at same time "to deny similar capabilities to the enemy".[58] The attack against the enemy's electronic systems is nothing new though. It is known that during Cold War, before the outbreak of hostilities, the first action expected was an Electromagnetic Pulse (EMP) which was supposed to destroy the electronic systems of the enemy, rendered them incapable of functioning. Billions of dollars were spent for EMP protected military systems.

10.8 Case Study: The Stuxnet Worm

Looking back at cyberwar's short history, with just a few shining examples, while Russia-Georgia short war in August 2008 showed cyber power's supporting role to that of the military, the cyberattacks against Estonia in April/May 2007, and even better the Stuxnet cyber incident against Iran proved that cyber power has already reached the point of an early maturity. The Estonia case proved that cyberwar against a nation-state, under certain conditions, in not a myth but it is real, here and now. Should we accept that the perpetrators of the attack were the Russians, then the political ends of the attack could very well be "show of force" in cyberspace,

[55] Betz, op. cit., p.24.

[56] Libicki, 2009, *op. cit.*

[57] *Ibid.*, p.140.

[58] Miller and Kuehl, *Cyberspace and the "First Battle" in 21st-century war.*

warning for future similar actions and punishment for actions incompatible with the interests of the perpetrator. The Stuxnet case, on the other hand, is an indication of the improvement of cyber capabilities, the higher ambition of political ends being able to be pursued and achieved through cyberwar and the autonomy achieved by cyber power vis-à-vis the other elements of power. The Stuxnet case is illustrative; we will use it as a case study to test the validity of our thoughts expressed above.

Stuxnet has been characterized as the first digital "fire and forget" precision-guided munition and perhaps the first peacetime act of cyberwar.[59] It is known neither when Stuxnet was launched nor who fabricated it. As for the latter, there are founded suspicions that it was a combined effort by American and Israeli scientists, with help from their German colleagues.

Though not explicitly declared, the political aim pursued in the case of Iran's nuclear programme by most of the international actors, with the USA as a front liner, is the cancelation of her nuclear programme. The available means for dealing with the problem are the elements of power, namely, diplomacy, economy and military power, with information in a clearly supporting role.

Options that could be implemented for the achievement of the aforementioned political aim consist of various combinations of the available means, each one with its own associated risk. Each of the options uses a primary element of power with the rest in supporting roles. The available options include (but are not restricted to) coercive diplomacy, economic sanctions, military power (in the form of bombardment, air strikes, use of Special Forces or even invasion of Iran) and cyberattacks.

The international community up to now has used diplomatic and economic means, supported by the threat of use of force (Israel is barely convinced by the USA to hold its plans to bomb the nuclear sites). Diplomacy as a primary means has obviously failed big time to produce the desired outcome and ultimately achieve the desired political end. Having failed to convince the Iranians to stop their nuclear programme, the international community escalated with economic sanctions in an attempt to coerce and compel them to do its will, while at the same time abandoning neither the diplomatic effort nor economic sanctions. The sanctions have been going on for some years now without obvious desired results. All this time, the military option was never off the table for the obvious reason to work in support of the other options. It is obvious, in this case, that the military option is the last resort.

As long as Iran continued to pursue its nuclear programme, the cancelation of the programme sought by the international community through diplomatic and economic sanctions was not achieved. The natural escalation would be the use of military power in the form of one or a series of raids (through air force, cruise missiles, Special Forces or a combination of the above) or even an invasion of the country, an option obviously expensive diplomatically and economically.

Before escalating to the use of military power though, some countries decided to use cyber power in the form of the Stuxnet worm. The use of cyber power proved to be a credible alternative option, cheaper and, more importantly, effective. Its use, with sanctions continued and a standing threat of use of force, bought for the international

[59] Milevski, *op. cit*.

community time, either for the sanctions to be given more time to work or for the military option to be better prepared, while at the same time showed the Iranians that escalation is a way forward, and at the end of that trail is the use of military power.

The Stuxnet operation was planned and executed at "state" (actually ad hoc alliance) level and had nothing to do with the application of military power. Therefore, cyber power was used at the level of the other elements of power, as a peer equivalent of diplomacy, economy and military power. Cyber power, in this case, offered an option in handling the crisis, short of war. Its effectiveness cannot be compared to that of military force, but the same applies to its cost, be it economic or human, and the impression to the rest of the world.

If grand strategy is the orchestration of all available elements of power for the achievement of a chosen political end, then we are in the middle of a full blown grand strategy with the use of all available elements of power, with primacy shifting progressively from diplomacy, to economy, to cyber power and, as last resort, to military power in pursue of the political end of cancelling or at least delaying Iran's nuclear programme. Among the elements of power, cyber power stands out as a cheap, easy to implement and rather effective means.

Lukas Milevski, although he sees the Stuxnet attack as "an instrument of strategy and policy", argues that it "may be judged a tactical success but a strategic failure".[60] In order for the attack to be called strategic success or failure, it should be judged against the political end for the achievement of which it was employed. Obviously it was judged that cyber power by itself was, for many reasons, insufficient to affect the Iranian political will to continue with its nuclear programme. Therefore, in this case, cyber power was used in concert with the other available elements of power with the purpose to delay (instead of abandoning) the nuclear programme, by causing physical damage to the nuclear facility. If the strategic objective was to cause damage and delay Iran's nuclear programme (as it seems most likely), then the attack was a strategic success; if on the other hand the aim was to coerce the Iranians to give up their nuclear programme for good, then it was a typical strategic failure of not matching "available means" to desired "ends". But this would be such an ambitious objective to be pursued; cyber power, with all its capabilities and the myth surrounding it, can achieve only so much. The strategic objective should not ignore the capabilities and limitations of the available means and should be adjusted accordingly. What Colin Gray reports for "military" applies easily to "cyber"; "The military means of war are, of course, vital, and they must be allowed to influence—even 'radically change'—the political aim".[61] "Estimates suggest that Stuxnet set Iran's nuclear programme back by several years"[62] and this was as much as Stuxnet could achieve, given all its current capabilities and limitations. As a side effect, which should not be overlooked, "Stuxnet must have had significant implications for Iranian morale as well due to the uncertainty surrounding the attack".[63]

[60] *Ibid*.

[61] Gray, *op. cit*., p. 30.

[62] Milevski, *op. cit*.

[63] *Ibid*., p.65.

10.9 Conclusion

With each passing day, dependence on cyberspace grows; there is no turning back to a world without it. On the other hand, with our ever-increasing use of, and reliance on, the Internet and digital technologies comes increased exposure, and vulnerability, to cyberthreats.[64]

Vulnerabilities are an inherent characteristic of every man-made system and cyberspace is not an exception. Those vulnerabilities, provided that they can be properly exploited, constitute the basis for the creation of an ever-expanding threat environment for human activities conducted within and through cyberspace. Cyberthreats early on drew the attention of nation-states, being a serious threat against their security, either in the wider sense on in its national security form. Therefore, defending cyberspace against cyberthreats became a priority for most governments. Since though cyberthreats transcend international borders, there is a growing need for co-operation amongst nations-states, private sector and academia to cope with it.

In parallel with the buildup of defensive capabilities for the protection of their cyberspace, governments, having realized that cyber power can be used for the achievement of political aims, develop their offensive capabilities and conduct offensive operations in cyberspace which in peacetime are limited to espionage and preparation for potential cyber conflicts. Given the current cyber capabilities, it seems that cyber power can by itself achieve limited political goals, making it thus a peer equivalent of the other elements of power of a state, namely, diplomacy, information, military and economy.

We cannot agree more with David Betz's argument that "cyber war is not coming",[65] albeit with a different meaning; cyberwar has already arrived; it is here and now! Given the current cyber capabilities though, it seems that cyber power can by itself achieve limited political goals, making it thus a peer equivalent of the other elements of power of a state, namely, diplomacy, information, military and economy. On the other hand, those capabilities, combined with the existing level of communication and information infrastructure of most state or non-state potential opponents, are not adequate to wage standalone cyberwar, except in limited scale and even then always combined with the threat of use of force.

Bibliography

Betz D (2011) Cyber war is not coming. Infinity Journal 3:21–24
Booth K (ed) (2005) Critical security studies and world politics. Lynne Rienner Publishers, London
Canada's cyber security strategy: for a stronger and more prosperous Canada, 2010
Castles S, Miller M (2009) The age of migration. The Guilford Press, New York

[64] New Zealand's cyber security strategy, June 2011.

[65] Betz, *op. cit*.

Caton J (2011) What do senior leaders need to know about cyberspace? In: Neal D et al (eds) Crosscutting issues in international transformation: interactions and innovations among people, organizations, processes, and technology, vol 11, Essay., pp 207–228
Clark W, Levin P (2009) Securing the information highway: how to enhance the United States' electronic defenses. Foreign Affairs, Nov/Dec 2009
Douhet G (1921) The command of the air. Office of Air Force History, Washington, DC, 1991
Farwell JP, Rohozinski R (2010) Stuxnet and the future of cyber war. Survival: Global Politics and Strategy 53(1):23–40
Goodman W (2010) Cyber deterrence: tougher in theory than in practice? Strategic Studies Quarterly Fall 2010:102–135
Gray CS (2013) Making strategic sense of cyber power: why the sky is not falling? Strategic Studies Institute, Carlisle, PA
Hathaway M, Klimburg A (2012) Preliminary considerations: on national cyber security. In: Klimburg A (ed) National cyber security: framework manual. NATO Cooperative Cyber Defense Center of Excellence, Tallinn, pp 1–43
Keymer E (2010) The cyber-war, Jane's Defence Weekly, No. 39, 29 Sept. 2010
Krepinevich AF (2012) Cyber warfare: a "nuclear option"? Center for Strategic and Budgetary Assessments, Washington, DC
Libicki MC (2009) Cyberdeterrence and cyberwar. RAND Corporation, Santa Monica, CA
Libicki MC (2011) Cyberwar as a confidence game. Strategic Studies Quarterly Spring 2011:132–146
Liff AP (2012) Cyberwar: a new 'absolute weapon'? The proliferation of cyberwarfare capabilities and interstate war. Journal of Strategic Studies 35(3):401–428
Lin HS (2010) Offensive cyber operations and the use of force. Journal of National Security Law and Policy 4:63–86
Lindstrom G, Luiijf E (2012) Political aims & policy methods. In: Klimburg A (ed) National cyber security: framework manual. NATO Cooperative Cyber Defense Center of Excellence, Tallinn, pp 54–65
Ludendorff E (1938) Total war
Luiijf E, Healey J (2012) Organizational structures and considerations. In: Klimburg A (ed) National cyber security: framework manual. NATO Cooperative Cyber Defense Center of Excellence, Tallinn, pp 108–145
Marinos L, Sfakianakis A (2012) ENISA threat landscape: responding to the evolving threat environment. European Network and Information Security Agency, Heraklion, Greece
Milevski L (2011) A special operation in cyberspace. Joint Forces Quarterly 63:64–69
Miller RA, Kuehl DT (2009) Cyberspace and the "First Battle" in 21st-century war. Center for Technology and National Security Policy, National Defense University, Defense Horizons, Washington, DC
Nadig A (2002) Human smuggling, national security, and refugee protection. Journal of Refugee Studies 15(1):1–25
Nye JS (2010) Cyber power. Harvard Kennedy School, Belfer Center for Science and International Affairs, Cambridge, MA
Steed D (2011) Cyber power and strategy: so what? Infinity Journal 2:21–24
Summers H (1982) On strategy: a critical analysis of the Vietnam War. The Random House Publishing Group, New York
UK Cabinet Office (2012) The UK cyber security strategy: protecting and promoting the UK in a digital world: 13-4
von Clausewitz C (1976) On war. Princeton University Press, Princeton, Edited and translated from German by Howard M and Paret P

Chapter 11
Cybersecurity in Europe: Cooperation and Investment

Pythagoras Petratos

Abstract European nations are subject to continuously increasing number and severity of cyber-attacks. In this essay we firstly examine the developments in cybersecurity and cyber-defence in Europe and particularly the European Union. The EU Cybersecurity Strategy is analysed. This is done in conjunction to the broader European Information and Communications Technology (ICT) agenda, as well as the Common Security and Defence Policy (CSDP), and related policies for cybercrime and intelligence. We identify common elements and especially the tendency towards more cooperation at various levels. This has spillover effects at international organizations as NATO and United Nation. The principal European Institutions associated to Cybersecurity are assessed. Except institutions the Defence and Security industry in Europe and the main challenges that faces are examined. The main hypothesis is if these policies and institutions can provide sufficient cybersecurity and cyber-defence. We conclude that Europe is on the right direction regarding cybersecurity and cyber-defence but it is questionable if these policies and institutions are backed by enough infrastructure and investment. Cooperation is crucial and can yield significant benefits. In that sense institutional overlap should be avoided and better coordination, sharing and pooling of resources, appropriate investment and infrastructure could significant mitigate risks in cyberspace and increase welfare.

Keywords NATO • Cyber-defence • NATO strategic concept • Smart defence • Interoperability • Tactics • Strategies

P. Petratos, Ph.D. (✉)
Saïd Business School, University of Oxford, Oxford, UK
e-mail: p.pythagoras@yahoo.com

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_11,

11.1 Introduction

The 4th of June 2013 was an important date for cybersecurity. In their first ever meeting dedicated to cybersecurity, NATO Defence Ministers agreed on the operational urgency of the Alliances' Cyber Defence Capability (North Atlantic Treaty Organisation 2013). The Secretary General emphasised the international nature of cybersecurity, "Cyber attacks do not stop at national borders. Our defences should not, either" and encouraged cooperation in an era of budgetary constraints "Defence budgets are falling, and the cost of modern capabilities is rising…. There is an imbalance between what we have and what we need…We must make the best use of the money we have, through better, smarter cooperation. And European countries must do more to relieve the unequal burden which is currently being carried by the United States" (North Atlantic Treaty Organisation 2013). The last sentence focuses on the role of European countries in cybersecurity. The purpose of this chapter is to analyse cybersecurity in the European context and to examine cooperation for more efficient investment and better cyberspace protection.

NATO and Europe, beyond their common membership, share another notable similarity: the cyberattack on Estonia in 2007. Estonia joined both the European Union and NATO in 2004. Estonia is an interesting case because it was previously on the western side of the Iron Curtain but most importantly due to the fact that it has a substantial Russian minority. Ethnic splits exist and the interethnic policies of ethnic Estonians can cause conflict with the Russophone minorities (Aalto 2003). It was exactly this type of tension that led to the well-known cyberattacks, which lasted for four weeks around May 2007. They were sparked by the decision to remove the statue of a Red Army soldier, which was related to the end of World War Two (Lannin & Mardiste 2008), from the center of the capital Tallinn. Russia, blamed for the attacks, denied involvement, despite an intense diplomatic row and the fact that some computer specialists found clues indicating that the attacks were linked to Russian government agencies' computers (Reuters 2007a). "NATO, partly prompted by the Estonian attacks, [formed] a cyber defence Centre of Excellence in Tallinn" (Lannin & Mardiste 2008) and, at the same time, the attacks served as a "wake-up call" for the European Union, according to EU Information Society commissioner, Viviane Reading (Reuters 2007b).

Indeed, this was a major incident and it was even labelled as cyberwar (BBC News 2007; Jenik 2009). It could be argued that the high-profile nature of this attack was mainly due to the involvement of Russia. It evoked the cloud of the Cold War and fears of escalation. The participation of states can also "typify a new battle tactic" (Finn 2007), signalling an innovative form of strategy, warfare or, ultimately, war. What is striking is that Estonia heavily used and relied upon digital infrastructure. The same is true of many countries, in particular because technology has continued to evolve since this cyberattack. The Internet has expanded considerably into mobile telephone use, banking, retail and many other aspects of modern life. Thus, the number of threatened assets has significantly increased. This is most evident in developed countries, where information technology has a growing number of

applications. It also applies to protecting vital public and private infrastructure, such as electricity grids and pipelines (Croft 2013), as well as critical information infrastructure (Commission of the European Communities 2009). This of course applies to European countries.

In our analysis, the focus is on member states of the European Union, because it has a well-defined set of policies and institutions. Given that context, we first analyse the EU policies related to cybersecurity. Specific attention is paid to the Common Security and Defence Policy (CSDP) and cooperation among EU member states. Then, the institutional setting connected to cybersecurity and cooperation is examined. We critically assess the ability of policies and institutions to respond to a rising demand for cybersecurity. Further, the discussion includes issues related to infrastructure protection, such as transportation and energy networks. Finally, we discuss governance, capacity building and cooperation in the European Union and how it can become "smarter" in order to deliver more value with respect to investment. The discussion also touches upon global governance surrounding the internet and cybersecurity.

11.1.1 European Cybersecurity Policies

11.1.1.1 Strategies

Information security in cyberspace is a multifaceted phenomenon. This is due to the fact that cybersecurity attacks can have an effect on many aspects of the European Union. Beyond the most obvious areas, such as information technology, foreign and security policy, justice and home affairs and the fight against fraud, information security can significantly affect various issues. The allegation in the summer of 2013 that the United States National Security Agency (NSA) bugged key senior European officials and intercepted emails has led to potential tensions in trade negotiations. This issue, which is linked to a leak by Edward Snowden, comes at a point when "Washington and Brussels are scheduled to open ambitious free trade talks next week following years of arduous preparation" (Traynor et al. 2013). In addition, German companies are concerned that the NSA may have stolen industrial secrets (DW 2013). Consequently, this could have an impact on EU issues such as enterprise, research, innovation, development and cooperation. Indeed, although the US is viewed as an ally, the European Union has threatened to suspend two data-sharing agreements, the Terrorist Finance Tracking Programme (TFTP), which passes information about international finance transfers to the US Treasury, and the Passenger Name Record agreement, which provide data on travel (Croft 2015).

Given this context, European policy should take into account the multidimensionality of information security. This is exactly what the new Cybersecurity Strategy by the High Representative Catherine Ashton and the European Commission attempts to achieve. It was publicised in February 2013 and is the "first comprehensive policy document" of the European Union in this area, pertaining to foreign

policy, justice, home affairs and internal market issues (EEAS 2013). The immediate reaction has been that this is a significant development and advancement. First of all, this is because the European Union recognises the importance of information security and acts accordingly. Second, the Cybersecurity Strategy addresses numerous vital issues such as finance, health, energy, transport, industry and, most importantly, economic growth resulting from making these activities secure. Finally, the document is rigorous in many ways. It is accompanied by a technical legislative proposal as well as an impact assessment covering different policy options.

Nevertheless, the most important element might be the characteristics it shares with other notable policies. There are significant commonalities with the new Strategic Concept by NATO. The "Comprehensive Approach" is certainly a principal resemblance. Both Strategies extent their foci on a broader range of issues and actors beyond the traditional approaches. Although it can be argued that the EU Cyber Security Strategy is more limited in its scope, this can be attributed to the limited nature of the issue. The most crucial element by far is the emphasis on international cooperation. The EU Cybersecurity Strategy calls for "improved coordination at [the] EU level" and facilitates collaboration by bringing together numerous actors such as law enforcement and judicial authorities as well as public and private stakeholders from within the EU, but in particular beyond its boundaries (EC 2013a, p. 10).

The document also suggests that the EU should address this global challenge with the relevant international partners, the private sector and civil society (EC 2013b, p. 14). The Communication broadens its mandate to EU external relations and Common Foreign and Security Policy (CFSP), confirming once again the comprehensive approach. Closer cooperation in this context encompasses organisations "that are active in this field such as the Council of Europe, OECD, UN, OSCE, NATO, AU, ASEAN and OAS. At the bilateral level, cooperation with the United States is particularly important and will be further developed, notably in the context of the EU-US Working Group on Cyber-Security and Cyber-Crime" (EC 2013b, p. 14). The analysis of EU relationships with these organisations is beyond the scope of this chapter. However, it should be noted that harmonious policy symbiosis is critical, because it would avoid friction in international relations and, at the same time, reap the likely benefits of cooperation.

In that sense, there is a high degree of consistency among different information security policies with respect to cooperation. The new Strategic Concept by NATO clearly mentions cybersecurity in particular as a more common emerging threat. At the same time, it recalls the "bonds Europe and North America [have]" and says that "the security of NATO members of both sides of the Atlantic is indivisible" (NATO 2010). It further states that the Alliance will engage in "cooperative security" through partnerships, especially with European democracies. This is a noteworthy development, because NATO not only reinforces cooperation with existing Allies but also focuses on expanding to additional European nations. These nations can participate in the accession process to membership in the European Union. It could be therefore said that the prerequisites for NATO partnerships pass through EU institutions. NATO can act as an additional layer to further deepen defense and

security cooperation in European nations. However, these processes are often simultaneous and can depend on idiosyncratic factors, thus possibly causing them to overlap.

At the level of the United Nations, the International Telecommunications Union (ITU) is the principal agency responsible for cybersecurity. Except for UN resolutions such as A/RES/57/239 and A/RES/64/211 on the global culture of cybersecurity, ITU recognizes its unique international character in the Global Cybersecurity Agenda (GCA). The 5th Pillar of the Global Cybersecurity Agenda focuses on international cooperation and global strategies at multiple policy levels. The central argument for the existence of this chapter is displayed in key documents such as the ITU National Cybersecurity Strategy Guide (2011). It re-emphasizes that "international cooperation [is] indispensable" and that "it is also important to involve other groups at the global level such as INTERPOL, NATO, OECD, IPU and UNDESA" (Wamala 2011). The similarities between European and ITU documents are remarkable. The ITU guide mentions that many countries may consider, as the United States does, promoting an international cybersecurity strategy. US policy is accurately reflected in the Department of Defense Strategy for Operating in Cyberspace, which is one of five strategic initiatives to build robust international relationships, as well as the US International Strategy for Cyberspace. Other countries present comparable strategies and activities for international cybersecurity cooperation.

In this part of the chapter, we presented the Cybersecurity Strategy of the European Union. It has critical features that are ripe for analysis. The first is that it expands beyond the traditional limits and has a "comprehensive" character. The second is the encouragement of international cooperation. Most notably, this trend exists in other cybersecurity strategies. Therefore, there is consistency between and momentum from numerous actors to enhance international cooperation for cybersecurity. In the following section, we proceed from wider strategies to narrower policies associated with cybersecurity and assess whether or not cooperation is also encouraged at these levels.

11.1.2 Other Policies

11.1.2.1 Digital Agenda for Europe

Cybersecurity in the European Union falls under the purview of the Digital Agenda for Europe (DAE). It is one of the seven key initiatives constituting the EU's strategy "to deliver smart sustainable and inclusive growth" (European Commission n.d.a). The DEA has seven pillars. The third pillar, titled "Trust and Security", proposes international coordination and a number of practical solutions organised into distinct Actions. These range from 28 to 41, including Actions 123, 124 and 125. Action 124 is the EU Cyber Security Strategy, while Action 123 proposes to incorporate it into law with the Directive on Network and Information Security. More specifically, Action 32 requires "stronger cooperation among Member States and the private

sector at national, European and international levels" (European Commission n.d.a) and Action 125 lists the activities of the European Commission for International Cooperation and the Global Alliance Against Child Abuse online. The Digital Agenda for Europe ends with an additional section titled "International", commenting that all of the seven pillars have international dimensions and that EU cooperates with many countries and international organisations in the digital domain. On Internet security "both bilateral and multilateral discussions and activities are underway, with the Commission actively engaged with the USA, China, India, Japan and other countries" (European Commission n.d.b).

11.1.2.2 Cybercrime

A distinguishing feature of the DAE is the discussion about cybercrime. Action 32 intends to fight cybercrime at the international level by strengthening cooperation among member states as well the private sector at the national and European levels (European Commission n.d.c). Moreover, it requires the consolidation of EU–USA international cooperation and further exploration of other strategic partners. This is another indication of the comprehensive approach encompassing home affairs. Police cooperation, as described by the European Commission, is law enforcement and intelligence sharing. It enhances cooperation through appropriate legislation such as the Swedish Initiative Framework Decision, the Prüm Treaty and the Prüm Decision (European Commission n.d.d). The main objective is to permit national law enforcement agencies to access and exchange information.

The evidence regarding police cooperation is mixed because there is limited information (Chatterton 2001). Bruggeman (2001) questions the ability and willingness to achieve police cooperation and internal security. In the same direction, Tak (2000) notes that there are three types of regulation and legislation that create bottlenecks to police cooperation in the EU. It can be argued that these bottlenecks might still exist, especially regarding violations of national sovereignty. Even with the implementation of the Third Pillar of the 1992 Treaty on the European Union, the 1997 Amsterdam Treaty and the 2001 Nice Treaty, there is criticism that these treaties' provisions lack clarity of focus and are very complicated (Skinner 2002). This argument is further elaborated by Friedrichs (2008) who argues that international police cooperation is a challenge to states, because it impinges on the legitimate use of force by states, which defines them in the Weberian tradition. Interestingly enough, Kierkegaard (2008) discusses the Prüm Decision through the lens of information security and although she recognises that it "represents progress in the field of cooperation", it touches upon sensitive areas with respect to privacy and data protection.

Beyond the legislative framework, there is a second element to police cooperation. It is the operational component. Of course, it should be said beforehand that operations are subject to laws, policies and practices. Deflem (2002) argues that despite the existence of successful operations under international cooperation, national interests dominate. Based on practices of European police cooperation,

Block (2008) concludes that "extensive and successful police cooperation does exist", but it is a complex field in which anecdotal evidence is not sufficient to present the broader picture. Although there are indications that cooperation is also progressing in legal cybersecurity frameworks, problems still remain for a "comprehensive approach" (Satola and Judy 2010).

11.1.2.3 Intelligence

A significant feature of cooperation in EU home affairs is intelligence. Lefebvre (2011) discusses international cooperation of civilian and intelligence agencies regarding terrorism. He recognises that Western security agencies have for a long time preferred to cooperate in a bilateral rather than a multilateral manner. However, there are notable examples of multinational cooperation such as the Club of Berne and the EU–NATO agreement.[1] Sir Stephen Lander, former Director General of the UK Security Service, states that "International intelligence cooperation is something of an oxymoron. Intelligence services and intelligence collection are at heart manifestations of individual state power and of national self-interest" (Lander 2004). This is a very strong assertion dismissing international cooperation and suggesting that the state remains in practise the principal actor.

On the other hand, Clough (2004) argues that national intelligence agencies do cooperate when benefits outweighs the costs, and identifies the trend toward the pooling of resources due to the cost of modern technology. Indeed, his argument that, in the European Defence market, some projects can be only realised through joint procurement is valid. Jennifer Simms (2006) advances this framework and uses an analytical perspective of cost-benefit analysis on intelligence liaisons. It is an important contribution analysing the mechanisms of intelligence cooperation. In addition, it can be applied to cybersecurity. This is due to the fact that often information on cyberspace has the characteristics of intelligence, utilised in strategic decisions.

The final aspect of intelligence is its connection to international relations. It has been argued that the role of intelligence in the context of international relations "is necessarily competitive, if not aggressive" (Lander 2004). Especially after the end of the Cold War, the clear distinction between the allies and foes of Western nations became blurred. It is not necessary to discuss the extended literature on the changing nature of international relations and intelligence. However, we should point out the fact that terrorism became an emerging global threat, especially after 9/11. Terrorism as well as other issues like organised crime has increased international intelligence cooperation.

The case of UK intelligence is worth mentioning. This is due to the UK's peculiar international relations context, encompassing its special relationship with US and its EU membership. Lander (2004) suggests that differences on the Iraq War

[1] "Agreement between the European Union and the North Atlantic Treaty Organization on the Security of Information," PESC 599, COSDP 463 (Brussels: 18 December 2002).

and the European perspective on the Balkans pushed the UK intelligence community toward schizophrenic tendencies; collaboration was possible on some issues, such as on terrorism, but there were no-go areas where tension in international relations existed. Aldrich (2004) highlights the effect of globalisation on intelligence liaisons and Svendsen (2008) connects intelligence with cooperation theory in international relations. Nevertheless, intelligence sharing does not only have clear implications for intelligence agencies and police but it could have spill-over effects to Common Defence and Security Policy (CSDP) (Agromaniz 2012). We extensively discussed the role of intelligence due to the fact that it involves valuable information and has been widely publicised due to the NSA case. In the next section, we expand on the international relations dimension of CSDP. We also analyse the defence and security policies related to cybersecurity in the CSDP framework.

11.1.2.4 Common Security and Defence Policy

The Treaty of Lisbon renamed European Security and Defence Policy (ESDP) to CSDP. It also created a High Representative of the Union for Foreign Affairs and Security Policy. Both were considered innovations, along with additional changes concerning the implementation of the Common Foreign and Security Policy (CSFP) (Europa 2010). In that sense, ESDP evolved to become a more coherent and visible policy intertwined with EU foreign policy. The abolition of the Second pillar, which constituted the CSFP before the Lisbon Treaty, generated a more integrated framework for external affairs and defence and security issues within the EU. With the abolition of the various pillars, the EU gained a legal personality that was before only a feature of the European Community, and, consequently, new rights at the international level. This provides the opportunity for the EU to act as a single entity on the international scene, joining international organisations and signing international agreements.

Another crucial change is the specific bridging clause, which applies to the whole of CFSP. While unanimity voting was inherited from previous treaties, the Lisbon treaty introduces some exceptions. Article 31 (ex article 23 of the Treaty on EU) describes four additional exceptions, which do not apply to decisions with military and defence implications.[2] This is one of the six Passerelle clauses that facilitate decision making and help to avoid deadlocks. As a result, the EU can respond more effectively to security challenges. Cybersecurity is a challenge as such. Due to the possible existence of asymmetric threats in cyberspace affecting some countries more than others, this process could prove quite beneficial. From a game theory perspective, countries with or without minimal risk of specific types of cyberattacks will not have an incentive to commit or invest resources to combat them. It could be argued that cyber terrorism is asymmetric among EU countries, with those more active in the fight against terrorism facing much higher risks. Thus, the specific

[2] Article 31, Lisbon Treaty.

bridging clause can have a significant impact on decisions about security actions at the EU level.

In addition, CSDP doubled the existing tasks from three to six, including joint disarmament operations, military advice and assistance tasks, and tasks in post-conflict stabilisation. Although cybersecurity might not be directly linked with these tasks, it can have an indirect contribution. Especially in post-conflict stabilisation, the creation of secure Information and Communications Technology (ICT) infrastructure is critical for economic development. Secure and reliable information is valuable for identifying illicit weapons during the disarmament process. The same applies to the prevention of conflict or terrorist attacks, and in assisting combat forces as well as a variety of operations. The theatre of operations has been transformed due to information technology (Smith 2003). In a network-centric operations environment, the security of communications, which often occur through the internet, is a necessary requirement in order to obtain superiority and avoid casualties and other negative effects. To sum up, the expansion of CSDP's defence and security tasks could increase the need for cybersecurity.

The Treaty of Lisbon significantly encourages cooperation. It has provisions on enhanced cooperation that include foreign and security issues. In addition, the general and specific provisions related to Common Foreign and Security Policy contain explicit cooperation actions. "The Union shall define and pursue common policies and actions, and shall work for a high degree of cooperation in all fields of international relations…".[3] This is probably the most important statement, calling for international relation policy harmonisation among member states. The usefulness lies in the fact that, with a coordinated foreign policy, the defence and security policies of the EU will reflect common objectives. Therefore, member states could pursue single EU goals rather than diverse aims, avoiding duplication of security capabilities and obtaining synergies. Other provisions include the strengthening of systematic cooperation between member states in the conduct of CSFP policy,[4] and the cooperation between the High Representative of the Union for Foreign Affairs and Security Policy and EU institutions, namely the Council and the Commission.[5]

What naturally follows from the above discussion is reflected on Article 24. It is the progressive creation of a common defence policy.[6] Later parts of this article declare that member states should work together to develop mutual political solidarity and, based upon it, conduct, define and implement CSFP.[7] The process of action convergence in the EU consists of consultation and coordination, not only within the EU but also between member states and their diplomatic missions on international organisations. These standpoints are represented in many parts of the Lisbon Treaty. Finally, attention should also be drawn to the extrovert character of the EU. The Union should develop relations and partnerships with global, international and

[3] Article 21, paragraph 2, Lisbon Treaty.

[4] Article 25, (c), Lisbon Treaty.

[5] Article 21, paragraph 3, Lisbon Treaty.

[6] Article 24, paragraph 1, Lisbon Treaty.

[7] Ibid., pp. 82-83.

regional organisations as well as other states, particularly in reference to the UN framework.[8] Cooperation at various levels, which we will analyse later, can have significant benefits. Thus, the Lisbon treaty contains critical provisions for cooperation on foreign and security issues, affecting the domain of cybersecurity.

11.1.2.5 Institutions

The previous section focused on policies related to cybersecurity. At this point, the institutional framework will be analysed. The effectiveness of EU institutions to provide sufficient security according to demand will be assessed and connected to investment. The most recent and important institutionalised security policy in the EU is the Common Security and Defence Policy (Hofman 2011). The analysis will start with an institutional analysis of CSDP and then progress to other institutions that have an impact on defence and security in Europe. Although the discussion is intended to concentrate on EU, it is essential to briefly describe the institutional overlap among EU, European and international institutions. This is because EU institutions do not remain unaffected by spillover effects from the activities of other institutions. Thus, in a globalised security environment of complex interdependencies, it is necessary to study the interactions between institutions.

Hofman (2011) argues that theoretical approaches to inter-institutional effects are in their infancy. Therefore, we prefer to avoid a theoretical analysis and rather aim to examine the practical implications for European cybersecurity. It can be argued that analogous overlap exists in the policy field. The increased density of international institutions and interactions between regimes (regime complex) imply that there is a parallel growth in norms, topics and policies (Raustiala and Victor 2004). Hence, it can be said that there is normally a process from institutions towards policies and their implementation. This is the reason for emphasising the role of institutions, which can consequently have, according to the literature, functional effects on policies and cooperation. A simple approach to studying these effects is a three-dimensional model of membership, mandate and resources (Hofmann 2009).[9]

In order to prioritize the analysis of institutions, the defence and security core is discussed first, after which we move to peripheral institutions. CSDP did not start

[8] Article 21, Lisbon Treaty.

[9] "*Membership* includes all formal members of international organisations, looking at various membership configurations that institutions offer states – such as the Partnership for Peace (PfP) in NATO. What matters is whether the state is included in the formal decision-making process. *Mandate* is understood as the tasks and functions that the institutions have subscribed to in their treaties, strategies and other constitutive and operational texts. Overlapping mandates imply that member states are subject to similar commitments. In the case of crisis management, the mandate can reach from low to high intensity crisis management operations or just elements of crisis management. *Resources* include the common and pooled resources of each institution. It stresses the fact that the existence of multiple institutions in one policy field increases the relative scarcity of resources." In Hofman (2011). Also see Hofmann (2009).

from nothing; it was based on ESDP (Cooper 2004). The "common European policy on security and defence" at the Cologne Summit in June 1999 was quickly formally renamed ESDP and later took its current form as CSDP under the Lisbon Treaty (Bickerton et al. 2011). The Saint Malo Declaration on December 1998 between the governments of France and the UK can be considered the trigger for the eventual realisation of the Amsterdam Treaty and further developments in EU defence and security. It is noteworthy that in the declaration, the Union has capacity for autonomous action, while at the same time acting in conformity with NATO. This was, and can still be, a point of friction. The relationship between the EU and NATO was "hotly debated" in both Saint Malo and Cologne meetings (Hofman 2011). Cornish and Edwards (2001) ask a number of questions regarding the EU–NATO relationship, such as "how autonomous" a European force could really be (Cornish and Edwards 2001).

Despite the mandate to fulfil the Amsterdam Treaty through ESDP, the Petersberg tasks were never fully, or at least to a satisfactory degree, realised. It should be noted that the Petersberg tasks date from 1992 and there was significant demand for them, particularly during the problems in the Balkans. This displays an evident weakness of the EU not only in failing to implement defence and security strategies and policies, but in failing to even create the respective institutions that the Treaty mandate required. If we assume that the Petersberg tasks demand an institution representing a proper European army, then they are a failure. It should be clarified that we are referring to the Helsinki Headline Goal and the capacity of the EU to deploy an army of 60,000 troops for up to 1 year at 60 days notice.

Of course, it should be acknowledged that the EU has conducted a wide range of missions globally (Gervi et al. 2009). There were 23 missions of ESDP till 2009, when the Lisbon Treaty came into force. These missions varied in numbers, reaching the considerable number of 7,000 personnel (Althea), and covered numerous tasks ranging from monitoring to police and military operations. Nevertheless, the occasions in which hard power was used, as in the case of Iraq and Afghanistan, are quite limited. There are two key questions arising from the above discussion with respect to cybersecurity. The first is a broader question. Does the EU have the capacity to conduct defence and security operations on a large scale? Would it even be able to approach the military capabilities required for the Petersberg tasks? This has significant implications for cybersecurity and cyberwarfare against powerful adversaries. The second question considers the quality dimension. Does the EU have the necessary means to secure communications? Moreover, would these operations be useful for learning by doing and increasing the knowledge and expertise of EU forces in cybersecurity? These two questions are interrelated, because there can be a trade-off between the quantity and quality of defence and security capabilities.

CSDP institutions have largely imitated NATO. The key institutions of the Common Security and Defence Policy, the Political and Security Committee (PSC), the European Union Military Committee (EUMC) and the European Union Military Staff (EUMS) were modeled based on NATO (Hofman 2011 This military institutional infrastructure was expanded to civilian affairs with the establishment of the Committee for Civilian Aspects of Crisis Management (CIVCOM) (Cross 2010).

From a quick examination, it seems that these institutions do not directly participate in cybersecurity per se. It could be argued that cybersecurity is a serious issue that has escaped the institutional "radar", because there has not yet been a significant crisis caused by the lack of cyberspace security. Some aspects of cybersecurity, such as intellectual property theft and everyday small-scale cyberattacks, can be ignored, for example, due to the fact that they do not qualify as major incidents or crises, or because it is very hard to identify and quantify their impact.

11.1.2.6 European Defence Agency

The European Defence Agency (EDA) is another principal institution. It is one of the newest EU agencies and its mission is to improve CSDP capabilities through cooperative European Defence projects in a time of budget constraints that stimulate the need for cooperation.[10] The European Union has increased its crisis management operations across the globe, as mentioned above, but defence cooperation remains ambiguous (Batora 2009). EDA functions in a policy environment that is characterised by high diversity and often competing visions of relevant institutional arrangements (Batora 2009, p. 1076). The density, diversity and overlap of institutions in the European defence and security environment can be fundamentally problematic.

The majority of literature on institutional overlap discusses international institutions. Nevertheless, the role of states is still critical. It should not be emphasised that defence and security budgets and other resources are basically controlled by EU member states. Contribution to EU or NATO missions is done on a voluntary base and there are a considerable number of cases in which member countries opted out or might not have contributed according to expectations. This is a manifestation of the free rider problem in alliances and can generate significant moral hazard caveats, which could in turn cripple trust and cooperation. Christopher Hill's (1993) argument was that EU capabilities were overhyped, to a level at which capability-expectations gap was created. As we discussed above, the EU has successful missions around the globe. However, it is doubtful whether it can meet the expectations and

[10]The EDA's exact mission: 'EDA's mission is to *support the Council and the Member States in their effort to improve the'European Union's defence capabilities for the Common Security and Defence Policy (CSDP).* This means running and supporting cooperative European defence projects; supporting research and technology development; boosting the European defence technological and industrial base; and providing a forum for European Ministries of Defence. EDA is one of the youngest European Union Agencies. It works on the basis of a new approach, tailored to the military needs of tomorrow, providing different and often innovative solutions. EDA and its participating Member States have launched important projects such as helicopters availability, the European Air Transport Fleet or the insertion of Unmanned Aircraft Systems into normal airspace, to name but a few. EDA is pragmatic, cost effective and results oriented. It offers multinational solutions for capability improvement in a time where defence budget constraints foster the need for cooperation.' It can be observed that it is primarily a cooperative institution in which all EU member states, but Denmark, participate. http://www.eda.europa.eu/Aboutus/Whatwedo/Missionandfunctions

perceptions of third parties to fulfill its international role, especially using hard power. Our argument does not only say that some countries could cover the deficit gap by contributing disproportionately to the rest of member states. A partial capabilities-expectations gap could exist if some states within the alliance were to not fulfil their obligations, at least to a sufficient level.

Batora (2009), in the context of EDA, argues that the defence spending of EU member states is often based on national priorities and lacks coordination in fields such as research and development (R&D) of new technologies and communications infrastructure. The latter is the underlying asset for cybersecurity. The Cyber Security Strategy of the European Union distinguishes cyber-defence as a dimension of cybersecurity. "Cyber defence is one of the ten priorities in the European Defence Agency (EDA) capability development plan (CDP). A project team of EDA and its participating Member States' (pMS) representatives is responsible for jointly developing these cyber defence capabilities within the EU common security and defence policy (CSDP)" (European Defence Agency 2013). There is an expert network conducting collaborative activities in order to deliver the required technologies on time. EDA is not only concerned with the military domain; it facilitates the creation of synergies among civil communities, national and European institutions, and NATO for the protection of critical cyber assets (European Defence Agency 2013, p. 1).

EDA concludes that the current state of cyber-defence in the EU (as of 2013) is at an early stage of maturity and provides recommendations. It splits them into two levels, the EU and Member States. For the EU level, it proposes, among other things, the development of a cooperation model among European institutions such as the European Network and Information Security Agency (ENISA) and the European Cybercrime Centre (EC3), a pan-institutional cybersecurity task force and the reinforcement of the relationship between the EU and NATO (European Defence Agency n.d.). Similarly for member states, EDA advocates the development of a cyber-defence doctrine and the evolution of organisational structures in coordination with other states, the exchange of information on equipment, recruitment, processes and pooling and sharing of facilities and cyber-defence capabilities. Finally, EDA has various cyber-defence projects encouraging cooperation. Training is done in close cooperation with NATO's Cooperative Cyber Defence Centre of Excellence (CCDCE). Situational awareness kits are developed along EUMS, US-led Multinational Capability Development Campaign (MCDC), and research and technology (R&T) platforms for further project collaboration (European Defence Agency 2013).

11.1.2.7 ENISA

In the previous paragraph, a fundamental European cybersecurity institution was mentioned: the European Network and Information Security Agency (ENISA). Its objective is to "to enhance the capability of the European Union, the EU Member States and the business community to prevent, address and respond to network and

information security problems. In order to achieve this goal, ENISA is a Centre of Expertise in network and information security and encourages cooperation between the public and private sectors" (European Union Agency for Network and Information Security n.d.). It is evident that ENISA's mandate is to encourage cooperation. Beyond facilitating cooperation among various actors in the information security field, it has distinct specialised units: the Computer Emergency Response Team (CERT), the Critical Information Infrastructure Protection (CIIP) and Resilience which is the identity and trust team, a hub for risk management and the key stakeholder-relations unit.

Although specialisation and cooperation are vital for European cybersecurity, questions regarding duplication of activities can arise. The obvious candidates are EDA and the Cooperative Cyber Defence Centre of Excellence (CCDCE). It should be acknowledged that both institutions concentrate on cyber-defence rather than the broader concept of cybersecurity. Especially in the area of Critical Information Infrastructure Protection (CIIP), the distinction between the two concepts is not clear because the same infrastructure can be used for many purposes. This is an example of how a definitional overlap might result in institutional overlap. Another issue is possible fragmentation. While the structure of European information security institutions avoids duplication to a certain degree,[11] this might cause coordination gaps and inefficiencies.[12] Stetter (2004), in an earlier study, confirms the complex and highly fragmented EU foreign-policy institutional architecture, and blames it for the decision-making that has led to a lack of leadership and has prevented comprehensive foreign policies with strategic directions from arising.[13] This is of major importance. Without clear strategic objectives, cooperation among EU member states might be unattainable or ineffective.[14] Institutional fragmentation is central to the reliability of critical infrastructure, such as telecommunications (De Bruijne 2006). In that sense, the scattered character of cybersecurity institutions and policies could have negative effects on the network security of critical information infrastructure.

The European Defence Agency identified the complexity of the numerous European institutions such as the European External Action Service (EAAS), the General Secretariat of the Council and European Commission, and related agencies like ENISA. It is beyond the scope of this chapter to unravel the decision-making processes of these institutions for CSFP, CSDP and cybersecurity issues. There are a variety of theoretical approaches analysing CSDP decision shaping and making, such as institutional dynamics (Gervi et al. 2009), inter-governmentalism (Hoffmann 1966; Moravcsik 1993), and trans-national networks (Slaughter 2004; Thurner and

[11] For example, the European Defence Agency supports the council and member states, while ENISA consults with the European Parliament regarding cybersecurity.

[12] Inefficiencies from transaction costs, opportunity, cost of time, and sub-optimal policies resulting from the complexity of decision making.

[13] In addition, Stetter expresses skepticism for the supranational-intergovernmental logic. This is also the opinion of Howorth (2012), presented in the next paragraph (Stetter 2004).

[14] This argument is analyzed later by using welfare economics and game theory.

Binder 2008), to name a few. Howorth (2012) concludes that the distinctions between major-EU decision-making agencies is blurred and that Member States still retain control in key policy areas, foreign policy and security being the most illustrative paradigm.

11.1.2.8 EUROPOL

The various policies for police and intelligence agencies cooperation were discussed above. The underlying institution facilitating these policies for better coordination and cooperation is the European Police Office (EUROPOL). It is the European Union's law enforcement agency. Its mission is to support member states in the prevention of and fight against all forms of serious international crime (Europol 2013a). The Lisbon Treaty and additional developments resulted in EUROPOL becoming an EU agency on 1st of January 2010 (Europol 2013b). Consequently, it moved to purpose-built headquarters and experienced an expansion in its capabilities.

Among the new capabilities, there is the formation of the Europol Cyber Crime Centre (EC3). Responding to increasing trends in cybercrime, the European Commission decided to establish this specialised center "to become the focal point in the EU's fight against cybercrime, through building operational and analytical capacity for investigations and cooperation with international partners in the pursuit of an EU free from cybercrime" (Europol 2013c). The first indication of cooperation is that EC3 shares the existing network and infrastructure of Europol (Europol 2013c). This is an illustrative example of efficiency gains from sharing resources and avoiding duplication.

The Europol Cyber Crime Centre is a cooperative body in its nature. It intends to provide collaborative responses in cooperation with EU Member States, but also key EU stakeholders, non-EU countries, international organisations, internet governance bodies and service providers, companies involved in internet security and the financial sector, academic experts, civil society organisations, National Computer, Emergency Response Teams (CERTs) and the CERT-EU (Europol 2013d). Moreover, the EC3 board has a diverse membership of eminent organisations in cybersecurity, including the following: specialised units, such as the European Union Cybercrime Taskforce (EUCTF), the Internet-Related Child Abusive Material Project (CIRCAMP), the European Cybercrime Training and Education Group (ECTEG) and the Computer Emergency Response Team (CERT-EU); other European specialised institutions, such as the European Network and Information Security Agency (ENISA), CEPOL (European Police College), and EUROJUST (European Union's Judicial Cooperation Unit); major European institutions like the European Commission and European External Action Service (EEAS); and the International Criminal Police Organization (INTERPOL). This is a very extensive and essential network for the fights against cybercrime.

However, the theoretical underpinnings should be tested in practice. Europol and EC3 have demonstrated some notable successes. As early as 2011, Europol

supported major cybercrime operations. Regarding different modes of cyberattacks, it was involved in operations Crossbill (malware) and Mariposa II (Butterfly bots). It also supported Operation Rescue, a highly publicised case against online child sex offenders, involving 14 countries with ongoing investigations (Europol 2013e). Operation Icarus, another case against online sex abuse, has identified 269 suspects and already 112 of them have been arrested across 22 European countries (InHope 2011). It can be said from these cases that Europol has acquired substantial technical and operational capabilities. In addition, the recently created EC3 in collaboration with the Spanish police dismantled a Russian-based cybercrime network. Operation Ransom involved a large and complex network infecting millions of computers and extracted profits from users in 33 different countries, 22 of which were European (Rial 2013). The prominence of the last case is not only a result of this success coming just one month after its establishment, but also due to the fact that it is a large international operation beyond the borders of the EU.[15]

Despite the successes of Europol and EC3 in combatting cybercrime, doubt arises regarding their capacity to have a decisive effect on cybercrime. Europol's capabilities cannot be compared at all with corresponding federal agencies like the Federal Bureau of Investigation (FBI). As of 2012, the FBI budget was $8.1 billion with 33,469 permanent positions (Mueller 2011), whereas Europol had a limited budget of approximately 84 million Euros and 800 employees (Europol 2013f). The size of cybercrime globally is estimated at $1 trillion and rising (Cameron 2011). It is therefore uncertain if Europol could manage to persistently pursue its goals at a reasonable level. It should be said, however, that EU policing is decentralised and states remain the main actors. Nevertheless, many of the member states lack sufficient cybercrime capabilities. Another issue is that the central coordinating authority and the periphery should have balanced power and capabilities in order to take advantage of synergistic effects. It is not useful to have national agents fighting international Trojan horse cyberattacks when no personnel (or too few) have the appropriate technical expertise to deal with it, and vice versa. It is a question related to Santiago's (2000) examination of whether the centralised model of information exchange of Europol is the most appropriate (Santiago 2000).

11.1.2.9 Defence and Security Industry

To make things even more complicated, the structure of the security and defence industry is a central factor. This happens for two reasons. The first is the relationship between the public and private sectors and the second occurs due to the association of state interests and domestic corporations. Fragmentation does apply to the European defence industry. Markusen (2008) suggests that mergers in the US defence industry consolidated the sector and Europe might move toward corresponding consolidation, international mergers and greater international cooperation

[15] It should be added that EC3 is expected to be fully operation by 2015. http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403457_text

(Markusen 2008). The dilemma for small European states and industries is more intense, because they face intense competition and economies of scale. Barros (2002), examining the case of the Portuguese defence industry, concludes that the only alternative is to opt out of European partnerships and participation in European joint projects; these results can be generalised to other small European countries.

After the end of the Cold War and the large decrease in defence spending and the approximately halving of defence sector jobs, the European defence industry seemed to be in a critical condition. At the beginning of the 21st century, it experienced a remarkable transformation. The European Defence industry, a collection of mid-sized, nationally oriented firms, became dominated by two giants and several other firms related to them (Guay and Callum 2002). ESDP and a general economic restructuring in the EU contributed to this transformation (Guay and Callum 2002, p. 757). It is then likely that CSDP could further enhance cooperation and mergers and acquisitions (M&A) activity in the European market. However, the sovereign debt crisis in Europe could provide both opportunities and challenges for the defence industry. It is still unclear what the impact of the crisis will be on the form of European economic architecture and government defence expenditures.

What is really striking is that cybersecurity has already had a profound effect on the defence industry. Despite the anticipated shrinkage of the US Defense Department due to budgetary constraints, a major Pentagon cybersecurity expansion was announced (Greenwald 2013). Indeed, it is this contrast that makes the case more notable. Whereas other parts of the Department of Defense (DoD) are likely to diminish, cybersecurity is expanding. This is not a strange phenomenon at all. The changing character of warfare with network-centric technologies, the technical change in the defence and security sector and, most importantly, the rise of novice cyberspace threats in number and sophistication, boost the demand for cybersecurity. The approximately fivefold expansion in personnel protecting critical computer networks includes the participation of the civilian sector.[16] It has the character of a public–private partnership. What is even more extraordinary is the funding associated with it. The Defense Department has already proposed an increase to $4.65 billion for the 2014 fiscal year from $3.94 billion in 2013, and this figure will be at this level until 2018, $23 billion in total (Capaccio 2013).

This is a clear signal of industrial restructuring. It is not only the considerable funds channeled to cyber-defence, but also the political commitments and strong statements drawing analogies to Weapons of Mass Destruction (WMD), 9/11 and Pearl Harbor. The defence industry is expected to react and it has done so, although it is still at an early phase. Numerous US defence contractors have been active in

[16] "The Pentagon has approved a major expansion of its cybersecurity force over the next several years, increasing its size more than fivefold to bolster the nation's ability to defend critical computer systems and conduct offensive computer operations against foreign adversaries, according to U.S. officials.

The move, requested by the head of the Defense Department's Cyber Command, is part of an effort to turn an organization that has focused largely on defensive measures into the equivalent of an Internet-era fighting force. The command, made up of about 900 personnel, will expand to include 4,900 troops and civilians" (Nakashima 2013).

cybersecurity. Lockheed Martin in 2012 won a contract valued at $4.6 billion for the management of the DoD's global data network, and ten cybersecurity centers have opened in Maryland, "the silicon valley of Cyber Security", since 2009, including companies such as Boeing Co., General Dynamics Corp. and Northrop Grumman Corp. It should be emphasised that beyond the traditional defence companies, there are a plethora of additional information technology corporations investing in cybersecurity, such as Cisco, Microsoft and Oracle, to name a few. This establishes a much broader cybersecurity nexus. All of the companies mentioned are incorporated in the USA.

Therefore, it can be argued that Europe has a considerable technological and industrial gap in the defence and information technology industries. As there is a trend towards the diminishment of the already relatively small (compared to the USA) European defence budgets, this gap is not likely to close any time soon. On the contrary, it is possibly going to widen. The information technology (IT) industry in Europe also lacks the innovation and size of the USA. Thus, the digital cybersecurity divide between the EU and the USA, ceteris paribus, would broaden. Although the USA is an ally rather than an adversary that could cause an arms race, EU member states should ponder whether their efforts are sufficient to combat cyber threats effectively. Consequently, this gap can cause free rider problems within NATO and transatlantic relations. To conclude, the European defence industry has made substantial progress following the fall of the Iron Curtain. However, significant inefficiencies exist in EU defence industries and their associated markets (Hartley 2010). In cybersecurity, this issue could be exacerbated because the IT industry in Europe is not as developed as that in USA.[17]

11.1.2.10 Investment in Cybersecurity

The Cybersecurity Strategy of the European Union calls for "Fostering R&D investments and innovation" (http://www.eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf). It will involve R&D for industrial policy support and the promotion of a trustworthy EU ICT industry, which would fill security gaps and prepare for new security challenges. Horizon 2020 is the EU framework programme for research and innovation totalling $ 80 billion and running from 2014 to 2020 (http://ec.europa.eu/research/horizon2020/index_en.cfm?pg=h2020). An important priority of Horizon 2020 is the EU International Strategy for Research and Innovation, ''a strategic and coherent approach to international cooperation" (http://ec.europa.eu/research/horizon2020/index_en.cfm?pg=h2020). One of the three objectives of international cooperation within the EU research and innovation context is the support for external policies and particularly CFSP. It is of major importance that CFSP and consequently CSDP constitute a principal priority. This would result in channelling of significant investment funds on these two broader policies and more specifically to cybersecurity.

[17] IT industries are developed in other countries, most notably China.

The Horizon 2020 is the EU reaction to increasing R&D investment by emerging economies as China, India and South Korea creating a global multipolar technology system. It should be noted that the countries mentioned possess substantial ICT infrastructure and industry. Thus, they are likely to have the capabilities to develop cyber capabilities. A question that follows this observation is if EU does invest enough in order to protect its infrastructure and retain and improve its competitiveness. An obvious comparison is the USA despite its limitations. The President's 2014 budget proposes investing $ 142.8 billion for Research and Development at the Federal level (http://www.whitehouse.gov/sites/default/files/microsites/ostp/2014_R&Dbudget_overview.pdf). We have already discussed the substantial funding of the US Department of Defense for cybersecurity. In addition the Department of Homeland Security is funded by $ 39 billion for critical capital needs for core commitments, one of them cybersecurity (http://www.whitehouse.gov/sites/default/files/omb/budget/fy2014/assets/homeland.pdf). Although EU state budgets have provisions for cybersecurity and related infrastructure investment is it quite doubtful if they reach, or even approach, the US levels. Nevertheless, the cybersecurity risks in EU and the USA share many similarities. It is beyond the scope of this chapter to analyse in detail and control for various factors in order to compare between the two regions.

In this comparison it is also important to examine the status quo. While EU can be considered to have better ICT infrastructure than emerging countries, it appears to have inferior infrastructure and capabilities than the USA. EU institutional capacity is also comparatively limited, as the case of Europol enlightening highlights. This is particularly true for Defence and Security, although significant steps are taken for its improvement. In addition the defence and IT industry in USA is considerably larger. Particularly many US technology companies after the financial crisis have massive cash that could be reinvested. The triptych of advanced status quo and institutional capacity accompanied by enhanced public and private investment in the USA can broaden the cybersecurity divide with Europe. At the same time there is pressure from other countries continuously increasing funding related to cybersecurity.

So the question is what would be the role of Europe and more specifically EU in global cybersecurity affairs? The balance of power in this area is shifting further. The recent NSA case displayed the weakness of EU even to be aware that it was under surveillance. At the same time other counties upgrade their cybersecurity infrastructure and capabilities. China is the most notable example with significant defence and security capabilities that became the second biggest defence spender after increasing its investment to more than $ 100 bn in 2012 (http://www.iiss.org/en/publications/strategic%20comments/sections/2013-a8b5/china--39-s-defence-spending--new-questions-e625). This is accompanied by global information and telecommunications companies such as Huawei Technologies Co. Ltd., Foxconn and Baidu and evidence of sophisticated of cyberattacks, as Aurora, tracing their origin in China. Non state actors, as terrorist groups and organised crime, could pose even more severe threats a decentralised multipolar cyber world.

Europe is in the right direction by adopting a comprehensive approach, increasing its institutional capacity for cybersecurity and starting to invest more in various

directions. This however might not be enough in order to maintain a leading global position. Enhanced investment targeting on synergies and efficiency, is necessary in an age of austerity, based on rigorous cost benefit analysis. This should come from both public and private sector, which could consolidate further. Cooperation is crucial. European nations can become more efficient and simultaneously increase their cybersecurity capabilities by appropriate cooperation. This however needs careful institutional design in order to augment incentives and avoid transaction costs and other type of negative spillover effects. Institutional overlap, unproductive coordination and duplication would cause problems. EU institutions should be organised accordingly and improve capacity building. ''Smart Defence" can be an effective solution. The use of existing cooperation structures, with the outstanding example of NATO, prioritising, pooling and sharing capabilities, could certainly constitute a strategy to mitigate the risks from cybersecurity and protect the wealth of nations and individuals.

References

Aalto P (2003) Revisiting the Security/Identity Puzzle in Russo-Estonian Relations. Journal of Peace Research 40(5):573–591

Agromaniz J (2012) A rhetorical spill-over? Exploring the link between the European Union Common Security and Defence Policy (CSDP) and the External Dimension in EU Counterterrorism. European Foreign Affairs Review 2(1):35–52

Aldrich R (2004) Transatlantic intelligence and security cooperation. International Affairs 80(4): 731–753

Barros C (2002) Small countries and the consolidation of the European defence industry: Portugal as a case study. Defence and Peace Economics 13(4):311–319

Batora J (2009) European defence agency: a flashpoint of institutional logics. West European Politics 32(6):1075–1098

BBC News (17 May 2007) Estonia hit by 'Moscow cyber war', BBC News Channel. http://news.bbc.co.uk/1/hi/world/europe/6665145.stm. Accessed 29 Nov 2013

Bickerton CJ et al (2011) Security co-operation beyond the nation-state: The EU's common security and defence policy. Journal of Common Market Studies 49(1):1–21

Block L (2008) Combating organized crime in Europe: practicalities of police cooperation. Policing 2(1):74–81

Bruggeman W (2001) International Law enforcement co-operation: a critical assessment. European Journal on Criminal Policy and Research 9(3):283–290

Cameron D (25 November 2011) Government publishes cyber security strategy. Prime Minister's Office, 10 Downing Street. https://www.gov.uk/government/news/government-publishes-cyber-security-strategy. Accessed 29 Nov 2013

Capaccio T (10 June 2013) Pentagon five-year cybersecurity plan seeks $23 billion. Bloomberg. http://www.bloomberg.com/news/2013-06-10/pentagon-five-year-cybersecurity-plan-seeks-23-billion.html. Accessed 29 Nov 2013

Chatterton M (2001) Reflections on international police cooperation: putting police cooperation in its place—an organizational perspective. In: Koenig D, Das D (eds) International police cooperation: a world perspective. Lexington, Lanham

Clough C (2004) Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation. International Journal of Intelligence and CounterIntelligence 17(4):601–613

Commission of the European Communities (30 March 2009) Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF. Accessed 29 Nov 2013

Cooper R (2004) Actors and witnesses. In: Gnesetto N (ed) EU security and defence: the first five years (1999–2004). Institute for Security Studies of the EU, Paris

Cornish P, Edwards G (2001) Beyond the EU/NATO dichotomy: the beginnings of the European strategic culture. International Affairs 77(3):587–603

Croft A (05 July 2015) EU threatens to suspend data-sharing with US over spying reports. Reuters. http://www.reuters.com/article/2013/07/05/usa-security-eu-idUSL5N0FB1YY20130705. Accessed 29 Nov 2013

Croft A (30 May 2013) Ministers to meet to review NATO's cyber defences. Reuters. http://uk.reuters.com/article/2013/05/30/net-us-nato-cybersecurity-idUSBRE94T0Z220130530. Accessed 29 Nov 2013

Cross M (2010) Co-operation by committee: the EU military committee and the committee on the civilian crisis management (Occasional Paper 82). EU Institute for Security Studies, Paris

De Bruijne M (2006) Networked reliability: institutional fragmentation and the reliability of service provision in critical infrastructures. Doctoral Thesis, TU Delft, Delft University of Technology

Deflem M (2002) Policing world society: historical foundations of international police cooperation. Oxford University Press, Oxford

DW (03 July 2013) Germany fears NSA stole industrial secrets. Economy. http://www.dw.de/germany-fears-nsa-stole-industrial-secrets/a-16925289. Accessed 29 Nov 2013

EC (2013a) Cybersecurity strategy of the European Union, Improved coordination at the EU level. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf, p. 10. Accessed 29 Nov 2013

EC (2013b) Cybersecurity strategy of the European Union, Improved coordination at the EU level. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf, p. 14. Accessed 29 Nov 2013

EEAS (2013) EU Cyber Security Strategy. http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm. Accessed 29 Nov 2013

Europa (26 April 2010) Common foreign and security policy. http://europa.eu/legislation_summaries/institutional_affairs/treaties/lisbon_treaty/ai0025_en.htm. Accessed 29 Nov 2013

European Commission (n.d.a) Digital agenda for Europe. http://ec.europa.eu/digital-agenda/digital-agenda-europe. Accessed 29 Nov 2013

European Commission (n.d.b). Digital agenda for Europe. https://ec.europa.eu/digital-agenda/node/54369. Accessed 29 Nov 2013

European Commission (n.d.c) Digital agenda for Europe, http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-32-strengthen-fight-against-cybercrime-and-cyber-attacks. Accessed 29 Nov 2013

European Commission (n.d.d) Digital Agenda for Europe, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/prum-decision/index_en.htm. Accessed 29 Nov 2013

European Defence Agency (2013) Cyber defence. Fact Sheet. EDA

European Defence Agency (n.d.) Homepage. http://www.eda.europa.eu/. Accessed 29 Nov 2013

European Union Agency for Network and Information Security (n.d.) Activities, http://www.enisa.europa.eu/about-enisa/activities. Accessed 29 Nov 2013

Europol (2013a) Europols priorities. https://www.europol.europa.eu/content/page/europol%E2%80%99s-priorities-145. Accessed 29 Nov 2013

Europol (2013b) Changing legal basis: steps to becoming an EU agency. https://www.europol.europa.eu/content/page/becoming-eu-agency-1859. Accessed 29 Nov 2013

Europol (2013c) A collective EU response to cybercrime. https://www.europol.europa.eu/ec3. Accessed 29 Nov 2013

Europol (2013d). Joining forces to catch the criminals. https://www.europol.europa.eu/ec3/joining-forces. Accessed 29 Nov 2013

Europol (2013e) Mandate. https://www.europol.europa.eu/content/page/mandate-119. Accessed 29 Nov 2013
Europol (2013f) Staff statistics. https://www.europol.europa.eu/content/page/staff-statistics-159. Accessed 29 Nov 2013
Finn P (19 May 2007) Cyber Attacks on Estonia Typify a new battle tactic. Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html. Accessed 29 Nov 2013
Friedrichs J (2008) Fighting terrorism and drugs: Europe and international police cooperation. Routledge, New York
Gervi G et al (2009) European security and defence policy: the first 10 years (1999-2009). The European Institute for Security Studies, Paris
Greenwald G (28 January 2013). Pentagon's new massive expansion of 'cyber-security' unit is about everything except defense. The Guardian. http://www.theguardian.com/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-stuxnet. Accessed 29 Nov 2013
Guay T, Callum R (2002) The Transformation and future prospects of Europe's Defence Industry. International Affairs 78(4):757–776
Hartley K (2010) The future of European defence policy: an economic perspective. Defence and Peace Economics 14(2):107–115
Hill C (1993) The capacity-expectations gap, or conceptualizing Europe's international role. Journal of Common Market Studies 31(3):306–328
Hoffmann S (1966) Obstinate or obsolete? The fate of the nation state and the case of Western Europe. Daedalus 95(Summer):892–908
Hofman S (2011) Why institutional overlap matters: CSDP in the European security architecture. JCMS: Journal of Common Market Studies, Special Issue: Security Cooperation beyond the Nation State: The EU's Common Security and Defence Policy 49(1):101–120
Hofmann S (2009) Overlapping institutions in the realm of international security: the case of NATO and ESDP. Perspective on Politics 7(1):45–52
Howorth J (2012) Decision making in security and defense policy: towards supranational intergovernmentalism*?* Cooperation and Conflict 47(4):433–453
InHope (16 Dec 2011) Europol—'Operation Icarus'—has identified 269 suspects and 112 suspects have been arrested in 22 countries. http://www.inhope.org/gns/news-and-events/news/11-12-16/Europol_-_Operation_Icarus_has_identified_269_suspects_and_112_suspects_have_been_arrested_in_22_countries.aspx. Accessed 29 Nov 2013
Jenik A (2009) Cyberwar in Estonia and The Middle East. Network Security 2009(4):4–6
Kierkegaard S (2008) The Prüm decision—an uncontrolled fishing expedition in 'Big Brother' Europe. Computer Law & Security Review 24(3):243–252
Lander S (2004) International intelligence cooperation: an inside perspective. Cambridge Review of International Affairs 17(3):481–493
Lannin P, Mardiste D (2008) Estonia wary of new cyber attacks. *Reuters*, April 7th
Lefebvre S (2011) The difficulties and dilemmas of international intelligence cooperation. International Journal of Intelligence and Counter Intelligence 16(4):527–542
Markusen A (2008) The economics of defence industry mergers and J c divestitures. Economic Affairs 17(4):28–32
Moravcsik A (1993) Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach. JCMS: Journal of Common Market Studies 31(4):473–524
Mueller R (April 06 2011) Statement before the house committee on appropriations, subcommittee on commerce, justice, science, and related agencies. http://www.fbi.gov/news/testimony/fbi-budget-for-fiscal-year-2012. Accessed 29 Nov 2013
Nakashima E (27 January 2013) Pentagon to boost cybersecurity force. Washington Post. http://articles.washingtonpost.com/2013-01-27/world/36583575_1_cyber-protection-forces-cyber-command-cybersecurity. Accessed 29 Nov 2013
NATO (Nov 2010) Strategic concept. http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf. Accessed 29 Nov 2013

North Atlantic Treaty Organisation (04 June 2013) Defence Ministers make progress on cyber protection. http://www.nato.int/cps/en/natolive/news_101143.htm Accessed 29 Nov 2013
Raustiala K, Victor D (2004) The regime complex for plant genetic resources. International Organization 58(2):277–309
Reuters (30 June 2007) Attack on Estonia puts cyber security on EU agenda. June 30th. http://www.reuters.com/article/2007/06/30/us-eu-digital-idUSL3044463420070630. Accessed 29 Nov 2013
Reuters (30 June 2007) Attack on Estonia puts cyber security on EU agenda. http://in.reuters.com/article/2008/04/07/idINIndia-32902120080407. Accessed 29 Nov 2013. http://www.reuters.com/article/2007/06/30/us-eu-digital-idUSL3044463420070630. Accessed 29 Nov 2013
Rial N (14 February 2013) European cybercrime centre dismantles its first criminal network. New Europe Online. http://www.neurope.eu/article/european-cybercrime-centre-dismantles-its-first-criminal-network. Accessed 29 Nov 2013
Santiago M (2000) Europol and police cooperation in Europe. Edwin Mellen, New York
Satola D, Judy H (2010) Towards a dynamic approach to enhancing international cooperation and collaboration in cybersecurity legal frameworks: reflections on the proceedings of the workshop on cybersecurity legal issues at the 2010 United Nations Internet Governance Forum. Wm Mitchell L Rev. 37, pp. 1745
Simms J (2006) Foreign intelligence liaison: devils, deals, and details. International Journal of Intelligence and CounterIntelligence 19(2):195–217
Skinner S (2002) Third pillar treaty provisions on police cooperation: has the EU bitten off more than it can chew? Colum J Eur L 8:203
Slaughter A (2004) A new world order. Princeton University Press, Princeton, NJ
Smith E (2003) Effects based operations. Applying network centric warfare in peace, crisis, and war. Office of the assistant secretary of defense, Washington DC Command and Control Research Program (CCRP)
Stetter S (2004) Cross-pillar politics: functional unity and institutional fragmentation of EU foreign policies. Journal of European Public Policy 11(4):720–739
Svendsen A (2008) The globalization of intelligence since 9/11: frameworks and operational parameters. Cambridge Review of International Affairs 21(1):129–144
Tak P (2000) Bottlenecks in international police and judicial cooperations in the EU. European Journal of Crime, Criminal Law and Criminal Justice 8(4):343–360
Thurner P, Binder M (2008) European Union transgovernmental networks: The emergence of a new political space beyond the nation-state? European Journal of Political Research 48(1): 80–106
Traynor I, Osborne L, Doward J. (30 June 2013) Key US-EU trade pact under threat after more NSA spying allegations. The Guardian. http://www.guardian.co.uk/world/2013/jun/30/nsa-spying-europe-claims-us-eu-trade. Accessed 29 Nov 2013
Wamala F (2011) The ITU National Cybersecurity Strategy Guide. International Telecommunications Union

Chapter 12
NATO's Cyber-Defence: A Methodology for Smart Defence

Marios Panagiotis Efthymiopoulos

Abstract The North Atlantic Treaty Organization, (NATO)'s Smart Defence policy, results as the allied decision towards the application of the Strategic concept. Its attempt for interoperable and technological evolution of its military forces and civilian assets is the added value that makes NATO's defence a smarter one: Agile forces command and tactical coordinated network-centric oriented operational capability. The ideological perspective of the political/legal framework is based on the necessity of a practical and renewed strategic concept. This concept was agreed initially in April of 2009 and adopted in 2010, considering the twenty-first century challenges and threats. By June 2014, NATO's "Smart Defence" policy is the newest "brand" name that agrees to agility of military and civilian capabilities at NATO. It is being applied at all levels in an innovative management way, including in the development of a joined cyber-defence policy. Smart Defence policy orientation is concentrated among others, to the constantly increasing need for a technologically secure environment for network centric operations but also deployment of forces. Cyber-defence can be used as a core smart defence policy. A coordinated level of tactical military and civilian capability and capacity deployment in tactical symmetric or asymmetric operations. This paper provides the reader with updated information on Cyber-defence policy, Smart Defence and the North Atlantic Alliance. It is an important topic of research that can hold an impact factor in practice. This paper is an analysis paper and examination paper. It looks at the "lessons learned" to this day. It recommends issues for future capacity management, administration and fiscal costs of cyber-defence in strategic networked operations.

Keywords NATO • Cyber-defence • NATO strategic concept • Smart defence • Interoperability • Tactics • Strategies

M.P. Efthymiopoulos (✉)
Harriman Institute, Columbia University & Strategy International,
New York, NY, USA
e-mail: marios.efthymiopoulos@strategyinternational.org; me2519@columbia.edu

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_12,

12.1 Introduction

In a research article on NATO's Cyber-defence, I argued that, "future war-like operations will be held in a far more complicated level of military operations"[1]. Current military operational and tactical needs, request good and agile capacities and capabilities of joined forces. Operations are conducted in a complex environment. Therefore the use of technology is a necessity, a tool for possible success. Operational deployment is interoperable and network-centric oriented. Technology as a tool is therefore an asset. Its capabilities are used for the success of military operations. Knowledge and good use of technology, and in specific cyber-defence are added values that minimise among others human cost.

The aforementioned issues are policy decisions. NATO leaders considered them when questions were raised on how to find a smart way to use technology. NATO, a peripheral international Organisation, a form of military supranational entity in the service of joined defence, agrees to the rules of the UN charter with respect to peace and breach of security. It falls under the framework of chapter VII[2] of the UN charter. It is a military security protection service provider, a 28 member state alliance, with a history that dates back to 1949 Washington Treaty. It provides a "military umbrella", an agenda of protection, from either external or internal, symmetrical or asymmetrical threats.[3]

In twenty-first century security affairs, NATO forces are required to be well prepared for possible rules of engagement. They should be able to counter symmetrical and asymmetrical battles and or threats or challenges. At this level of preparedness, scenarios, of possible attacks and battles that can be anticipated are methods of and for action. They are seen as methods for preparation that could be applicable at possible military action.

The use and necessity today of technology is limitless. So is the virtual world of defence, where technology and cyber-defence 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-assaults, where counter-measures are needed.

Since the adoption of the NATO Cyber-Defence policy,[4] NATO is in the middle of both training and action. NATO is constantly training its forces on Cyber defence. Training can be achieved through national, bilateral even multilateral levels of NATO, through the association of member states, at the level of Centres of Excellence, such as the CCD COE.[5] Training is anticipated to increase, while NATO

[1] Efthymiopoulos MP (2008) *NATO's Security Operations in Electronic Warfare: the policy of cyber-defense and the alliance new strategic concept*, Australia. (Journal of Information Warfare) JIW Vol. 8, Issue 3. http://www.jinfowar.com/.

[2] Charter of the United Nations, Chapter VII: action with respect to threats to the peace, breaches of the peace, and acts of aggression. http://www.un.org/en/documents/charter/chapter7.shtml.

[3] UN Charter & NATO Atlantic Treaty, Washington DC, USA, 1949.

[4] NATO's Cyber-Defense Policy (2011) http://www.nato.int/cps/en/natolive/topics_78170.htm.

[5] NATO Cyber-Defence Centre for Excellence. https://www.ccdcoe.org/.

gets more engaged in the field of cyber-defence, in both operations and tactics. It is anticipated that NATO is by now well prepared, both for current and future challenges, countering multiple and multileveled dimensions of cyberattacks. Yet it also holds an open option to if necessary, conduct counter-offensives to prevent further escalation of cyber or military actions.[6]

Missions of NATO, "will continue to require agile and interoperable, well-trained and well-led military forces".[7] The new technological and operational environment through cyber-defence, provides NATO with a new level of technological possibilities; new tools for use against possible threats but also protective "cyber-objectives". Allies now have an added policy, mission and value, concerning its ongoing and constant transformation to reach capabilities and political excellency. NATO aims for well-coordinated missions with other international organisations as well, when prompted to react in international threats or challenges. As such we should clearly state that NATO has the ability and future potential of, what we may call it, as the "online" security protection initiative against all possibly known threats. Now it seeks excellency in achieving the best smartest way to protect but also counter-attack. By "nature" NATO aims to prevent attacks. Through small and 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-defence capabilities in a smart way, is the "operative goal". NATO members prepare well and at joint levels. NATO's Smart Defence,[8] a policy framework for defence tactical advice and operations, is the method that among others brands the need for a cyber-defence policy. What Smart Defence stands for, we approach in details below. 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" [9]—meaning not only defensive-clause operations but also counter-offensive operations.[10] Cyber-protection as such is needed when defence of allies is associated with possible threats or challenges.

In this analysis paper, we will argue that there is an increasing need to adopt newer and better methods and actions that are innovative, for successful application of a Cyber-Defence policy that protects well member-states. A correctly applied and enabled NATO Cyber-Defence policy with fully agile and capable joined forces

[6] Hughes RB (2009) Atlantisch Perspectief, Ap:2009 Nr. 1/4, *NATO and Cyber-Defense: Mission Accomplished, Netherlands, Netherlands Atlantic Committee.*

[7] Ibid. 1.

[8] 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.

[9] Sendmeyer SA (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.

[10] NATO (2008) *Briefing on Transforming Allied Forces for Current and Future Operations*, NATO Public Diplomacy Division, Brussels.

command, will counter successfully possible current and new, symmetrical and asymmetrical threats.

This paper examines the ever enlarged process of ongoing training/preparations and constant challenges raised through the framework of NATO's cybersecurity and defence. The purpose of this article is to draw attention to the future of, what and how, when and in what other dimension, will military operations be conducted. In what level of approach and therefore what preparation should we use. This paper posits that most future, defensive or offensive battles, will occur in a continued asymmetric mode of conduct—as was the case with the cyberattacks in Estonia in 2007[11] and as such a strong smart cyber-defence "umbrella" is needed.

This article stresses in short, that NATO Cyber-Defence policy, should never stop transforming, while technology progresses and threats expand to a new and deep digitised world of insecurity. There is a need of a policy method approach for continued practical allied update and practical preparation to counter cyberattacks. Innovative methodology and ideologies are needed to process such a policy approach. In turn a strong and smarter that the current one, preparatory policy applied, will better prepare member states and NATO forces for possible electronic warfare. Interoperability of forces for joint use in cyber-defence should be achieved. NATO should "e-volve" as should Allied "e-networked" States. NATO should innovate and manage. NATO should administer change on methods of smart defence in cyber-defence, through constant cyber-research, cooperation strategically and technically.

I finally stress that the issues analysed and proposed in this article are sole opinions of the author and are not related in any official way with the organisation or governments. They represent academic analysis that is shaped from primary and secondary sources of information. Arguments are solely based on personal academic research, experience, judgments and cooperation established in the framework of this current research.

The issues presented hence forth, are for consideration. They solely reflect the operational and tactical levels of what NATO needs to be at the level of cyber-defence.

12.2 NATO's Smart Defence and the Correlation with Cyber-Defence Policy

In an international and interconnected environment that is full of challenges and threats, in times of austerity and historical geographical political changes, smart defence, a policy for renewal that is of "political essence" of and for Alliance unity, has come forth. It was presented to the NATO Summit of the 28 members, heads of

[11] Scheherazade Rehman (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.

state and government in Chicago.[12] It will be evaluated at the upcoming NATO Summit in Wales' Celtic Manor Resort, Newport in the UK in September of 2014.[13]

Smart defence is a new security culture comprehension. It is a new way of thinking. It is all about generating modern defence capabilities at all levels. It is all about new ideas. It is all about the future of NATO as an alliance in practice. It is about the encouragement of cooperative defence. It is about maintaining military capacities and enhancing military capabilities.

According to the new strategic concept, NATO is moving forward. twenty-first century needs and challenges require agile and compatible forces at all levels, including network-centric operations and defence. NATO forces cannot be static in terms of progress of tools for use for defence purposes. NATO needs to have interoperable, capable and well equipped technological forces. Smart budget, directed funds include the capacity for building and planning the effectiveness and operational viability of forces, with minimum budgets and costs, with enhanced technology and minimum engagement of human assets in both time and operations. Smart Defence is all about renewing operational and tactical effectiveness; operational alliance coordination; It is all about specialisation of forces. Smart Defence is sets priorities better coordination through collective efforts and good use of technology, innovation and knowledge.

Smart Defence is about geopolitical capability and capacity of implementation; it is all about area distribution and specialisation with minimum cost. It is a correlation of administrative political and military coordinating joined bodies within NATO. Member states and NATO should not continue to duplicate procedures and efforts on subjects and policies such as Ballistic Missile Defence, Intelligence, Surveillance, Reconnaissance, Cyber-defence, Maintenance of readiness, training and force preparation as well as effective engagement; All this should be expected to work with minimum cost, casualties and high level of technology preparedness that is both beneficial and practical.

Smart Defence is a priority policy for NATO. It is the continued evolution of the capabilities initiative, one that also includes the examination, purpose, evaluation and application of and in cyber-defence. It aligns supranationalised national capability priorities with those of NATO. Its policies on standing management of operations, is a cooperative and consensus levelled agreement; it is a way that produces a cost-effective projection, planning and application for the theatre of operations in the real and virtual worlds.

Specialisation is a key word for success in the attempt to hold smart capabilities and policies. It is the essence for coordinated efforts while lowering cost, fiscal and human. It increases joint cooperation, effectiveness. It guarantees national engagement of states to NATO policies, when correctly pointed out. Specialisation is a form of cooperation that engages geographical interests, strategic sharing of costs, technological information and intelligence.

[12] NATO Chicago Summit: http://www.chicagonato.org/.

[13] "NATO Secretary General in London for talks of the Wales Summit": http://www.nato.int/cps/en/natolive/news_106833.htm.

Smart Defence is a long-term viable solution through which NATO Defence Ministers have paved the way for a "branded" success. During the Chicago Summit, elements for Smart Defence and Cyber-Defence cooperation were addressed. Overall, a package was negotiated and agreed. The concept on Smart Defence was adopted and is now expected to rise up to the level of awaited outcomes at all operational and training levels. It will possibly be evaluated in the forthcoming NATO summit meeting in Wales UK in 2014. A levelled evaluation will result to a new approach, a new commitment, a new mindset of capabilities and effective engagement in policies such as cyber-defence at various levels of preparedness and action at the theatre of operations.

Smart Defence is a political and military concept within the overall Strategic Concept of NATO; a new security culture understanding. It is a "macro-political" application with long-term solutions at various agenda levels, such as the one explored in this article. Smart Defence means reapprochement of collective understanding for a new Euro-Atlantic posture and a new Euro-Atlantic identity and fidelity that is yet to be developed in practice and at all levels of capacity reach.

12.3 How is Smart Defence Associated with Cyber-Defence? "Engaging Through Policy Orientation"

Practically, still not much has been achieved at the overall level of Smart Defence capabilities. The inability and/or unwillingness of member states, for political and military national engagement has to now be confronted, mainly as fiscal austerity measures are applied and cutbacks are in effect.[14]

Heads of state and governments however do listen and observe. Although Smart Defence as a policy, renders cheaper the cost for the total sharing of burden by member states, not all members share the same burden to this day, as also the cost differs from state to state. Unfortunately, in a time of austerity measures and political challenges and changes, states are yet to realise how cost can be measured, in smart budget 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. The tools therefore will have to be evaluated so as well future operations in terms of smart cos, while making sure that human cost will also be lowered considering the increased use of technology as a tool and method.

While, national and collective defence remains at the forefront of interests of states, a new "reapprochement" is needed among member states. Cyber-defence as key core policy for smart defence can attract attention for stake holders. Through communication and marketing perspectives, social media and workshops, conferences cyber-defence should continue to be promoted and have a clear aim.

[14] 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 Illinois, USA.

Cyber-defence, a core policy in Smart Defence works as a "decree of specialization for each member state". States will chose, at what level to invest and which levels to approach. In it, cyber-defence policy must and should always be provided as a tool. It is and will always be a tool for a joint framework of cooperation, globally. The best and most attractive action is one that binds together as many members as possible. However, we should also stress that for cybersecurity to succeed, countries should understand that they need to offer together, equally balanced assets. National and supranational infrastructures as such will be complemented and protected. Cyber-defence is profitable. Its fiscal cost of envisioned support should be clarified as are its outcomes. Its feasibility and profitability study should also be shown.

As Smart Defence is being upgraded and developed, Cyber-defence, not a conception but a real-politic issue, should become not only a tool for specialisation policy but also a key for concrete engagement of all member states. It will render a policy of unity (political) success towards NATO and its future as an organisation.

Cyber-defence and technological progress within NATO, can therefore be seen as the core and Smart defence core policy for NATO. It is innovative. It provides technological architecture and posture. It can provide robust deliverables with minimum human capital, fiscal and technical cost. It will hold a global reach of success eventually. It will market NATO in the "smartest and easiest way" in the twenty-first century, in as well existing now emerging markets and associated states with NATO counting more than 62 countries to this day.

12.4 NATO's Cyber and Security Policies Environment in 2014

Latest research has reveals that NATO's policies and its security environment have been assessed.[15] In a post-2001 terrorist era in 2014, the Alliance has among others:

1. Invoked article 5,[16] claiming its right to defence against external aggression,
2. Allied states agreed on an everlasting transformation, politically, militarily, operationally and strategically in Prague 2002,
3. Agreed to be involved in outer-areas of traditional operations Kosovo,[17] Afghanistan in 2001[18] onwards via operation International Assistance Force[19] and by the end of 2014 end operations.

---

[15] Efthymiopoulos MP (2008) *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).

[16] NATO (1949) *NATO Treaty: Basic Document of the Treaty*: http://www.nato.int/docu/basictxt/treaty.htm#Art05.

[17] NATO (1999) *Operation Allied Force on Kosovo*: http://www.nato.int/issues/kosovo_air/index.html.

[18] **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**.**

[19] NATO (2001) *International Security Assistance Force (ISAF)*: http://www.nato.int/isaf/index.html.

4. Has agreed on Smart Defence initiative of qualitative and quantitate value, of joint interoperability efforts, including efforts on Cyber-Defence[20].

Considering aforementioned political decisions, one important issue comes out. NATO is a necessity. As such NATO should now be branded smartly. Such actions reaffirmed by the Heads of States, include among others, the Treaty of London in 1990 Summit, to the 1994 Summit in Brussels, and in 1999 over its 50th year anniversary Summit in Washington, to the immediate decisions taken in 2001 after the terrorist acts in the USA [21] to its 60th anniversary, which was held in Strasbourg and Kiehl accordingly in April 2009 to the Chicago Summit in 2012 add value that states the following: NATO was created for a long-term and therefore it is here to remain. Now while it evolves, it is being "rebranded" and re-organised to face threats and challenges ahead.

In its administrative form, operationally and tactically I consider NATO to be: "…the purest form of a true military-political alliance that brings and binds together member countries that hold the same supranational interests, in terms of security, in all related fields, such as military, political, financial, sociological and environmental security"[22] affairs. Now I project that we should include the topic of cyber-defence and technology to this framework of interests and commands.

Allied member states, in 2002, agreed that NATO was required to change politically, militarily, administratively, through a conceptual joined decision process. This process of change was decided and initiated at the Alliance summit meeting in Prague. The reason was clear: the constantly challenging security environment and future threats to emerge. At the turn of the century, NATO's 2001 Strategic Dogma was again seen to be re-evaluated and a new one possibly considered. It was widely challenged by member-states that not enough was done. Some say, it was no longer viable considering the terror events in 2001. Others considered NATO's 2001 Strategic Concept as a step, a strong basis that would create future constant collective changes, a newly established enlargement process and the creation of new policy ideas. It was seen as an opportunity, for restructuring a renewed concept more practical that would later lead to the policy of Smart Defence engagement NATO members in reaching better capabilities through joined programmes of interest as was the use of technology for defence purposes.

Smart Defence in turn would lead to the following:

- A concept and later a Smart-Defence policy and possibly a cyber-defence core policy, that would portray all practical political and military needs but was not yet anticipated as an idea or procedure, yet foresighted from the twenty-first century security instability environment;

[20] Ibid 4.

[21] NATO (2001) *Information on immediate NATO reaction*: http://www.nato.int/docu/update/2001/0910/index-e.htm.

[22] Ibid 1.

- NATO's Strategic Concept of Security in turn clarified policies, operational needs and expectations, both at tactical and operational levels, providing clear roads for manoeuvring.
- Finally the concept allowed for a clear statement on a smarter evolution on capabilities. Capabilities when specialised would render the necessary financial but also legal clauses, for operational smart preparation and success while lowering human capital and leading the way into twenty-first "technological revolution".

The renewed Concept of Security was agreed to reflect an agreement that would practically be applied at all levels of NATO. The decision for evaluation, consultation and drafting the New Concept of Security of NATO was held at the NATO Heads of State and Governments, Summit meeting in Strasbourg-Kiehl on April 3rd and 4th.[23] The outcome would result to the Lisbon Summit meeting in Portugal in 2010,[24] where the new concept of security would be adopted.

The Alliance would now be able to deliver better and more robust results to twenty-first century security challenges. 14 years in the twenty-first century, NATO would continue to transform but now would also operation not within the limits of its political decisions (that should be widened) and boundaries, but rather according to its own "rules of engagement" (NATO's military doctrine, that would include the protection, use and defence through the cyber-world, providing NATO with side, unlimited abilities for action. It is widely believed, that the Alliance has now the ability to operate in a largely different security environment that is no longer limited only to symmetrical threats or geographical areas but also to an environment of asymmetrical threats in an e-world areas of interest. NATO has the capability and capacity to counter-fight any opponents by military men-led operations whether in the real world or the cyber-world. In supporting components in land, air and sea power in an out of controlled area operation NATO can among other issues provide cyber-defence. It is capable of support led, peace-keeping, or peace-making operations, and counter-intelligence, counter-attack and cyber-defence concept operations.

12.4.1 Trends In An e-Security World

It is believed that the twenty-first century will be a century, where all matters will be dealt through the use of advanced technology. In our year 2014, technology is a tool that we are interconnected with, as are services provided through the Internet. Our wired-society that includes online services, such as banking, communications, security services, shopping and media-services to name a few, take place by now in cyberspace. These services are by now vulnerable to cyberattacks. As countries

[23] NATO Kiehl-Strasbourg Summit meeting: http://www.nato.int/cps/en/natolive/news_52837.htm?mode=pressrelease.

[24] Lisbon Summit Declaration: http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease.

steadily move forward in becoming dependent on technology and wider networks, security stakes also increase.

Current security risk assessments consider that there is constant development of cyber-organised crimes that need to be countered. "Cybercrimes" are executed by organised groups. Hackers are considered illegal users that know how to get access to personal, classified or other unauthorised information by informal and unaccepted ways at all levels and in all places. The use of personal, unauthorised or private information to get access to other resources such as funds or weapons access is a crime, as is the use of the Web to terrorise citizens, states, institutions or organisations.

In terms of applying these issues in military policy, through national or NATO command on cyber-defence 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-Defence policy was in fact a necessity, and more importantly, was seen as a necessity that we clearly pointed out following the first truly organised cyberattacks in Estonia in 2007.[25]

12.4.2 NATO's Concept of Cyber-Defence

NATO's Military Committee decided on what has come to be called as a "Cyber-Defence Concept". The Committee's aim is to deliver practical results that will point out: (1) the necessity of NATO as a collective organisation in a globalised and currently unsafe e-world, and (2) the Alliance' ability to deliver new policy results, taking into perspective new forms of asymmetrical threats such as cyberattacks.

Historically, the 2002 Prague Summit first marked NATO's tasking authority committee with regards to all activities that should be held in relations to Cyber-Defence. As technical achievements were delivered, so policy-makers delivered policy results on Cyber-Defence. 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 cyberattacks by new forms and means developed by NATO's Allied Command Transformation (ACT) In Norfolk Virginia.

In turn, the Informal Meeting of the Ministers of Defence in October 2007 output for NATO,[26] gave way to the inauguration of NATO's centre of excellence (COE), the Allied Command Transformation on Cyber-Defence, in Estonia that named the Centre the CCDCOE.[27] It was based on the Concept of Cyber-Defence, as agreed by NATO's Military Committee.

---

[25] Cyber-Policy in Estonia: http://www.nato.int/cps/en/natolive/75747.htm.

[26] NATO Defence Ministers Meeting (2007) *Informal meeting of NATO Defence Ministers*: http://www.nato.int/docu/comm/2007/0710-noordwijk/0710-mod.htm.

[27] NATO (2008) *CCDCOE*, URL: from: http://www.ccdcoe.org/11.html.

The central and final decision-making role over the policy of cyber-defence, however, is the North Atlantic Council (NAC), which is the highest deciding political authority. It considers NATO's policies and activities in regards to political and military affairs. Below the NAC, is NATO's Consultation Control and Command Agency (NC3A) [28] and the NATO Military Authorities (NMA). The latter authority has implementation as its major task [29].

The implementation of NATO's Cyber-Defence 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".[30] 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.[31]

NATO's policy creation and activity is encouraged by the Alliance to engage as many as possible governments, if not all member-states of the Alliance, but also industries relating with these matters. In accordance to its best practice policy, NATO considers that its "operational forum" can and should be considered as the best joint operational co-operation between states, as to also avoid duplication of efforts.

Practically, in military policy, implementation or operational areas, there are "three phases of practical activity": in its initial phase a NATO Computer Incident Response Capability (NCIRC) was established as well as its "interim operating capability". Its second phase involved an ever more realistic and pragmatic perspective that required the coordination of all initial "offering" states (under the NATO agreement between states of a voluntary national contribution—VNC), in bringing the NCIRC to a full operational capability [32].

New policies came about after being proposed and coming to effect (well-known procedure of internal NATO working process). A so-called "Memorandum of Understanding" was drafted and proposed to NATO by the sponsoring state, in this case Estonia, prior to any of the above-mentioned phases of practical activity.

From that point on, it is the administrative decision of the Alliance, that once the aforementioned stages are put into effect, then a third phase comes into turn. Needless to say, this third phase may also be the most important. 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 has been evaluated, then the Allied Command Transformation (ACT)

[28] NATO NC3A (2002) *NC3A Agency*, URL: http://www.nc3a.nato.int/Pages/Home.aspx.

[29] NATO's Cyber-Defence policy, (2008d), *Defending against cyber-attacks*, Focus Areas: http://www.ccdcoe.org/37.html.

[30] NATO (2009) *A Road Map to the Strategic Concept of NATO*: http://www.nato.int/strategic-concept/index.html.

[31] NATO (2008) *NATO Defence Against Cyber Attacks*: http://www.nato.int/issues/cyber_defence/practice.html.

[32] Ibid.

decides whether to declare the operational centre—in this case the Cooperative Cyber Defence (CCD) COE (Estonia), what is called as a "Centre of Excellence". The outcome in May 2008 was that the centre of CCD in Estonia was declared by NATO Allied Command Transformation as a "Centre of Excellence" (CCDCOE).

12.4.3 Cyber-Defence Put into 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 centre, which was to be yet supported by other states as well. It had applied, as a newcomer, to the Alliance, to establish the first operational international military centre ever, in its history, as a NATO Ally. (2) Estonia had already been witness of modern asymmetrical warfare attacks in 2007. This came as a result of Estonians removing the bronze statue of a Red Army soldier from the centre of Tallinn an honorary statue honouring the dead of the Second World War. This matter sparked social outrage between the 60–65 % of its Russian Speaking, Russian native population and the Estonian Government (News Scientist 2007). It resulted to continuous cyberattacks on Estonia's e-infrastructure public or private, military or civilian. One year later in 2008, seven countries according to the memorandum of understanding, helped Estonia get full operational capability (Germany Italy, Latvia, Lithuania, Slovakia and Spain), which lead to its current status. By the summer of 2009 Status was supposed to include also the possibility of the USA, which initially was interested in Joining; Turkey and Greece were by the summer of 2009, initiating an evaluation of their needs on whether or not to join this centre. By 2014, NATO is now engaged as is the centre with the training and preparation of Non-Member states, outsourcing in essence its capacities in states that are in need in sharing information and knowledge such as in Moldova,[33] led by the country of Belgium.

The cyberattacks in Estonia, the biggest one and the most organised electronic attack, with a duration period of several weeks, provided NATO with a motive and multipurpose task for the years that would have to come. NATO's leadership was in fact correct in its judgment that: (1) Such an operational centre and policy was needed (2) Its operational centre would constantly be evaluating and evaluated. Would research on prospective evolutions in technology, malware and cybersecurity.

Since the inauguration of its Co-operative Cyber-Defence Centre of Excellence (CCDCOE) in Tallinn Estonia in May 2008, the centre initiated a mission and a vision statement. 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

[33] Sharing Malware information to defeat cyber-attacks: http://www.nato.int/cps/en/natolive/news_105485.htm.

interoperability in the field of cooperative Cyber-Defence". Its vision is to be "a primary source of subject matter expertise for NATO in cooperative cyber-defence related matters".[34]

The domain of cooperative cyber-defence, focus areas of research include:

- "Legal and Policy
- Concepts and Strategy
- Tactical Environment
- Critical Information Infrastructure Protection"[35]

Core policy is created by research and policy-orientation seen above. As a procedure it is presented primarily to the Supreme Commander Allied Command Transformation (SACT), by a request of NATO HQ (Head Quarters) and by the North Atlantic Council (NAC) level. This includes: Doctrine and Concept Development, Awareness and Training, Research and Development Analysis and Lessons learned and finally Consultation.

12.4.4 NATO Approaches Issues Relevant to CyberSecurity

For the concept of Cyber-Defence, the Centre for Excellence in Tallinn continues to portray NATO's need for the creation of a permanent, core policy at the level by now of Smart Defence. On February 6th and 7th 2009, NATO's Science for Peace and Security (SPS) sponsored a workshop that would foresight our statement that cyber-security approach and cyber-defence is a core policy. The workshop was titled "Operational Network Intelligence: Today and tomorrow". Its overall purpose as stated was "to rethink present strategies and identify urgent measures to be taken in order to minimise the strategic and economic impacts of cyber-attacks".[36] This was the level of anticipation for the future correlation of Smart-Defence with the policy of Cyber-defence at its core. And at this level we now anticipate by 2014 UK Wales summit to evaluate and consider the possibility of Cyber-defence becoming the core objective of Smart defence.

NATO increasingly recognises that organised cyberattacks seek to take advantage as is stated *modern society's dependence on sophisticated technology in order to inflict serious damage on economies and national security*. NATO as observed over years of primary research both at professional and academic levels, is also of firm belief that there is an increasing need for the coordination of the human factors related to the issues of electronic warfare, operational network, intelligence, Cyber-Defence… and maybe soon to come in smart robotics and smart soldier protection shield.

---

[34] Ibid 27.

[35] Ibid 29.

[36] NATO (2009) *SPS workshop rethinks approaches to cyber security*: http://www.nato.int/docu/update/2009/02-february/e0206a.html.

NATO is currently using people involved in e-systems, security, IT engineers, researches, officers dealing with network operations and operational centres as well as professional and academics. NATO estimates, that they should be systematically involved at organised levels of research, sharing, discussion and exhibition of outcomes, which will in turn enrich the abilities, capabilities and capacities of rendering current smart-defence and cyber-defence as a key and successful policy.

12.5 Proposals

NATO's level of ambition on the policy of Cyber-Defence and at the general policy of electronic warfare should increase, through the overview policy framework of Smart Defence.

Current professional and academic military and technological led research should coordinate itself with practical work made at NATOs military operational levels. Said that, NATO should and could do more on this matter in the short-term by:

1. Sharing more information on all affairs of Cyber-defence within and among member states but also non-NATO members but cooperative states.
2. NATO should continue to apply possible outcomes coming from the Centre of Excellence at a tactical level but also operational levels of NATO.
3. NATO should make a clearer budget on smart defence based on the technological necessities that allow lower but shared budgets for the long-term and a policy of cyber-defence that look operationally and market-oriented more attractive, as NATO cannot reach the interoperability levels, through "analogic" of capacity building of forces.
4. By joined co-operation at the level of electronic-warfare prevention, detection and reaction to attacks towards member allied states, duplication of policy can be avoided if only nations share together and act together in unite under NATO's joined Smart-Defence policy and the policy of cyber-defence at its core.
5. A legal proposal on what constitutes an e-crime or e-terrorist attack should be clarified if not yet done so.
6. The capability or capacity for NATO to operate in an e-world should be also clarified in accordance to the policy of Smart-Defence policy recommendations and needs, while NATO still attempts to reach "excellency" of capabilities and interoperability of forces.

In the long-term NATO needs to do the following:

1. Adopt new policies relating to practical operational and tactical guidelines for future warfare. A foresight on smart soldiers and smart attackers should be created.
2. Tallinn's CCDCOE should continue be supported for the upgrading and the creation of a purely military NATO operational centre on electronic warfare (NATOCEW) that will deal with the application of current CCDCOE research. It will progress all operational levels of interoperable cybernetic preparation of forces for all purposes of engagement of forces in electronic warfare.

3. NATO should enhance its national protection plan of major infrastructure through the total cooperation of national states.
4. NATO base infrastructures should also be constantly protected from fraudulent attacks.

12.6 Concluding Remarks

In conclusion, the main aim was to portray a relatively new but important issue that has been developed conceptually and practically by NATO Allies. The aim was to project the important of the matter. The creation of a Concept of Cyber-Defence and the inauguration of the Centre of Excellence for Cyber-Defence in Tallinn Estonia, according to the decision of the SACT at Norfolk Virginia, provided an impetus for future operations but also administrative and operational upgrading in the field of today's smart defence policy a result of the renewed strategic concept. Cyber-defence is a policy within the framework of NATO, yet it is not a key core policy just yet. This article aimed to show why cyber-defence should become a core policy for NATO and for allies. The article conceptualised issues at a policy concentration, it analysed the policy of smart defence and cybersecurity and defence while strategically looking to the growing necessity for constant protection against current of future challenges and threats. The article projected examples and forward to this proposals were pointed out.

The policy of Cyber-Defence through the prism of Smart Defence allows for truly and united allied effective engagement practically in military operating environments at all levels; offers shared co-operation. While the process of Internet use develops in a more smart way NATO should seek legal advice and set up an international legal scale in the wideness need of operations that should reflect and allow to operate well beyond its borders, so as to make sure that no attacks remained unanswered.

This paper provided the reader with updated information on cyber-defence policy, Smart Defence and the North Atlantic Alliance. It is an important topic of research that looked at the "lessons learned" to this day. It recommended issues for consideration and future capacity management, administration, fiscal costs, operational methods, of cyber-defence in strategic networked operations.

Chapter 13
The Security Culture of a Global and Multileveled Cybersecurity

Zenonas Tziarras

Abstract This paper seeks to argue for the development of a global and multileveled management of cybersecurity. To do so we first define cybersecurity by situating it within the broader framework of the changing concept of security. To this end we look at the evolution of the security concept, mainly since the end of the Cold War, and its relationship to cybersecurity in today's global affairs. Then we identify the referent object of security, the importance of cyberthreats, and the need for a multileveled management of cybersecurity and cyberthreats. For such a management to be possible and effective, this paper argues that the development of a security culture of multileveled cybersecurity is necessary. To demonstrate how that could happen policy-wise, we briefly look at the current state of international cooperation on cybersecurity and put forward the idea of a framework of multileveled and global cooperation based on a strategy aiming at developing a global security culture of cybersecurity. Moreover, it is suggested that the development of this security culture should be gradual, based on horizontal and vertical multileveled cooperation, by starting with "low-politics" or non-politically sensitive cybersecurity matters. Such a multileveled framework of cybersecurity, with successful communication lines on and between all levels, may even provide a good platform for cooperation in other domains as well.

Keywords Cybersecurity • Cyberspace • Cyber-Defense • Security culture • Strategy

Z. Tziarras (✉)
Department of Politics and International Studies, University of Warwick,
Coventry CV4 7AL, UK
e-mail: z.tziarras@warwick.ac.uk; ztziarras@strategyinternational.org

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_13,

13.1 Introduction

Technology has become the main driver of globalization. Indeed, we could speak of economic or cultural globalization but the reason why national economies and cultures have been integrating more and more is not free trade or multiculturalism-oriented policies. Time and space have shrunk because of the evolution of technology and everything that comes with it. Likewise, every means of transportation has been a product of technological advancement. Today, the rapid increase in global human interactions, financial transactions, international cooperation, and the increasing importance of non-state actors in global affairs, has become possible and easy through the use of information or cyber technology. In other words, the emergence of cyberspace has created a whole new world and dimension which is nonetheless interlinked with practices and actors of everyday life. In this context, Anthony Giddens's argument that globalization is "the intensification of worldwide social relations that link distant localities in a way that local happenings are shaped by events occurring many miles away and vice versa," becomes even more relevant almost two and a half decades later.[1]

But how should we then approach security and cybersecurity thus dealing with cyberthreats more effectively? This paper seeks to argue for the development of a global multileveled management of cybersecurity. To do so we first need to define cybersecurity by situating it within the broader framework of the changing concept of security. To this end we look at the evolution of the security concept mainly since the end of the Cold War and its relationship to cybersecurity in today's global affairs. Then we identify the referent object of security, the importance of cyberthreats, and the need for a multileveled management of cybersecurity and cyberthreats. For such a management to be possible and effective this paper advocates for the development of a security culture of multileveled cybersecurity. To demonstrate how that could happen policy-wise we briefly look at the current state of international cooperation on cybersecurity and put forward the idea of a framework of multileveled and global cooperation based on a strategy aiming at developing a global security culture of cybersecurity.

13.2 On (Cyber) Security

Admittedly, security is an essential element in everyone's life. Given the fact that security and insecurity affect people's lives every day, one could easily comprehend the extent to which they matter in global politics and international relations. However, the end of the Cold War complicated the discussion about the concept of security as it created a new global security environment which has been constantly

[1] Anthony Giddens, *The Consequences of Modernity* (Cambridge: Polity Press, 1990). 64.

changing since then. Thus, security has become a contested concept with definitions ranging from national and international security to human security.

The term "International Security" first appeared during the Cold War and used to have a much narrower meaning than it does today.[2] One could easily understand why during the Cold War the prevailing concept of (International) Security was "strategy." Not only was security understood within the framework of strategy, but that turned out to be the concept on which the theory of (neo) Realism was based. Neorealism, and therefore security, was used to be expressed through four key elements: "state, strategy, science and the status quo;" these are still some of the main characteristics of Realist theory.[3] This concept of security and the theory of Realism were clearly relevant during the Cold War while one could argue that the global political realities of that period could only be understood through the 'Realist' concept of International Security. The major competition between the two superpowers of the international system, the arms race, and the fear of a potential nuclear war were some of the main features that characterized the Cold War and influenced the foreign policy-making of the USA, the Soviet Union, and their allies. In that sense, the most cherished value during the Cold War was—national and international—peace as it was the most threatened value.

As noted earlier, the prevalent understanding of security during the Cold War was seriously challenged after the end of bipolarity. The collapse of the Soviet Union gave an end to the narrow idea of strategy and military as the main security concept and made room for new threats to enter the debate of how security should be addressed and conceptualized. A small taste of how broad this discussion became is not only the inclusion of new threats that emerged in the post-Cold War era but also the emergence of a debate about whether security is a sub-field of International Relations and vice versa.[4] Regardless of the relationship between Security Studies and International Relations, strategy is today perceived only as a sub-field of security and not as a synonym to it. What broadened the field of security after the Cold War were factors that concern demilitarization, the spread of democracy, the evolution of technology and communications and, therefore, the 'increasing globalization'.[5]

This essay adopts Williams's proposed understanding of security as the most relevant and valid one: "security is most commonly associated with the alleviation of threats to cherished values; especially those which, if left unchecked, threaten the survival of a particular referent object in the near future."[6] We also accept that given

[2] Stephen M. Walt, "The Renaissance of Security Studies," *International Studies Quarterly* 35, no. 2 (1991): 213–14.

[3] Paul D. Williams, "Security Studies: An Introduction," in *Security Studies*: *an Introduction* ed. Paul D. Williams (New York: Routledge, 2010), 3.

[4] Terry Terriff et al., *Security Studies Today* (Cambridge: Polity, 2006). 12.

[5] Iztok Prezelj, "Challenges in Conceptualizing and Providing Human Security," *HUMSEC Journal* no. 2 (2008): 2.

[6] Williams, "Security Studies: An Introduction," 5. Williams' definitions draws upon similar previous definitions such as Wolfers'; see, Arnold Wolfers, "National Security' as an Ambiguous Symbol," *Political Science Quarterly* 67, no. 4 (1952): 485.

the changes in the international system after the Cold War, a wider security agenda is justified and rather helpful to our understanding of new threats, such as cyber-threats; yet the military and the 'Realist' dimensions of security should not be entirely supplanted. Drawing upon the literature on security studies there are certain questions that we could ask in order to narrow down what the "cherished values" and "threats" are, as well as how to "alleviate" these threats. These could be concisely expressed in the following four questions[7]:

(a) What is the referent object of security?
(b) What is the security threat?
(c) Who is responsible for providing the security?
(d) Which are the best ways to provide security?

Answering these questions can help us understand the importance of cybersecurity and the ways in which a security culture of multileveled cybersecurity could be formulated.

13.2.1 Referent Object(s) and Cherished Values

The referent object of security during the Cold War, as we have already seen, was the state. In other words the "state" was the object that was primarily threatened and had to be secured. Later, within the framework of the widening security agenda, the security of the individual and its well-being had become increasingly important. Further, the significance of the strong relationship between the state and the individual has been underpinned by a large body of literature creating a whole new dimension of security and human security in particular.[8] As such it has been argued that the security of individuals is directly linked to national security and therefore it should be prioritized "since without reference to individual humans, security makes no sense."[9] Emphasis has been given on many other referent objects as well; after all, as Baldwing states, "the choice depends on the particular research question to be addressed"[10] and, as one could argue, on who sets the security agenda. What would then the referent object of a multileveled cybersecurity be?

[7] Wolfers, "'National Security' as an Ambiguous Symbol."; David A. Baldwin, "The Concept of Security," *Review of International Studies* 23(1997): 13–17; Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2010). 10–13; Williams, "Security Studies: An Introduction," 5–10.

[8] Richard H. Ullman, "Redefining Security," *International Security* 8, no. 1 (1983): 130–31.

[9] Williams, "Security Studies: An Introduction," 7. Williams cites, Ken Booth, "Security and Emancipation," *Review of International Studies* 17, no. 4 (1991); and, Bill McSweeney, *Security, Identity and Interests*: *A Sociology of International Relations* (Cambridge: Cambridge University Press, 1999). 45–68.

[10] Baldwin, "The Concept of Security," 13.

We argue here that in order for a security culture of multileveled cybersecurity to be possible, multiple referent objects need to be taken into account. In this context cyber(in)security should be addressed at the individual/societal, national/state, regional, and international level. All these—often interlinked—levels constitute our security referent objects. As cyberspace has created a "parallel universe" in which all these levels coexist at all times and in relation to all aspects of social, political and economic life, then, it is against this background that cyber insecurity should be addressed. At this point one could argue that Nye may indeed be right in that "cyberspace is not a [global] commons like the high seas because parts of it are under sovereign control."[11] But in a globalized world, where there is increasing interconnectedness on every level, a legitimate argument could be made that cyberspace should become a single—though multileveled—referent object. Accordingly, cyberspace should be protected on every level as the cherished values (interests) at stake are not only individual but collective as well. This levels-of-analysis approach is similar to that of Choucri: drawing upon the "fourth image"/global level put forward by Robert North,[12] Choucri suggests that "Cyberspace allows both the constrains and the opportunities rooted at the local level to extend within and across levels of analysis nearly unimpeded and to circulate through the global system."[13]

13.2.2 Cybersecurity Threat(s)

Having established the referent object of (cyber) security and its relationship to cherished values, the next step is to decide what constitutes a threat. According to the referent object (e.g., states, individuals, social groups), cherished values vary[14] and, therefore, we should decide which of these "values are threatened and by what or whom."[15] In other words, security threats are—and arguably should be—mainly perceived according to what one considers the referent object to be. It should also be kept in mind that (human) "security is directly related to the concept of international peace and security;"[16] as such, some threat agendas are more important than others in terms of their political significance, or depending on the significance of the one who sets the agenda.[17] For example, the threat agenda of the UN High-Level Panel on Threats, Challenges and Change is probably more significant than any other

[11] Joseph S. Nye, *The Future of Power* (New York: Public Affairs, 2011). 143.

[12] Robert C. North, *War*, *Peace*, *Survival*: *Global Politics and Conceptual Synthesis* (Boulder, CO: Westview Press, 1990).

[13] Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge: The MIT Press, 2012). 46, 44–48.

[14] Baldwin, "The Concept of Security," 13–14.

[15] Williams, "Security Studies: An Introduction," 8.

[16] Prezelj, "Challenges in Conceptualizing and Providing Human Security," 9.

[17] Williams, "Security Studies: An Introduction," 8.

agenda in international politics.[18] Also the threats presented in it are undoubtedly the ones that the international community will care the most about—albeit their ranking is debatable.

Importantly enough cyberthreats were not included in the list of the 2004 UN High-Level Panel, although one could categorize them under "Terrorism." Yet cyberthreats vary in nature and cannot be limited to cyberterrorism. Choucri identifies "three broad types of cyber contentions and conflicts: contentions over the architecture of the internet and the management of cyberspace, conflicts in the pursuit of political advantage and economic gain (legal and illegal), and cyber threats to national security." Under these broad types fall, for example, cyberthreats to infrastructure (e.g., communications and information), to national security, and political or commercial cyberthreats to individuals, firms, governments, and states.[19] Nye focuses on national security and sees four main cyberthreats: "economic espionage, crime, cyberwar, and cyberterrorism."[20] On the other hand, Rosenfield argues that "cybernetic warfare and the threat it poses to modern society" needs to be redefined. He goes on to emphasize that the "disruptive potential of cybernetic attacks" is more threatening than their "destructive potential" while he divides cyberattacks into "two principal forms: those targeting data and those targeting control systems." Rosenfield adds that most cyberattacks are related to data targeting, "from online credit-card fraud to Web site vandalism to large-scale denial-of-service (DOS) assaults."[21]

It is clear that every day-life practices are not only as threatened as national security but perhaps even more so. In this context the various types of cyber-threats could directly or indirectly affect multiple aspects of social, political, and economic life through the "disruption" or "destruction" of critical infrastructures. A paper of the European Commission, in 2005, clearly stated that "Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments."[22] From that perspective cyber-threats are directly associated with human, national, international and, therefore, global (in) security as they are essentially converted into other types of threats once they take place; such threats include economic, food, health, environmental, community, personal, and demographic threats, among others.[23] In Davies's words "The informa-

[18] Panyarachun A et al., "A More Secure World: Our Shared Responsibility," (High-Level Panel on Threats, Challenges and Change: United Nations, 2004), 21–59. The ten main security threats identified were: poverty, infectious disease, environmental degradation, interstate war, civil war, genocide, other—war related—atrocities, weapons of mass destruction, terrorism, and transnational organized crime.

[19] Choucri, *Cyberpolitics in International Relations*: 126, 25–53.

[20] Nye, *The Future of Power*: 144.

[21] Daniel K. Rosenfield, "Rethinking Cyber War," *Critical Review* 21, no. 1 (2009): 77–78.

[22] EC, "Green Paper: On a European Programme for Critical Infrastructure Protection," *Commission of the European Communities* COM(2005) 576(2005): 20.

[23] Prezelj, "Challenges in Conceptualizing and Providing Human Security," 8, 17.

tion technology infrastructure is at risk not only from disruptions and intrusions, but also from serious attacks."[24] Such attacks, intrusions and disruptions could have a great negative and costly impact on areas such as international banking, military systems, governmental systems, local businesses, communications, transportation, and many others. It is thus clear that cybersecurity is of the essence for literally everyone—even if they do not own a personal computer—as the cherished values of any given referent object are potentially under threat.

13.2.3 Security Provider(s) and Policies

The last two questions to be answered are rather interlinked as the ways (policies) of providing security are not only directly related to the referent object and the security threats but to the security provider as well. Security providers may vary in size, influence and importance, especially within the framework of international relations and global politics. In that light, the security provider could be the state, an international organization, a non-state actor or even individuals with certain power capabilities and in certain situations.[25] To be sure, depending on the security threat, some security providers are more capable of managing certain threats than others. On the other hand, a particular agent might not care for a security threat as much as another agent would[26]; therefore, as a broadened threat agenda becomes gradually necessary the need for different actors or agents to address particular threats arises as well.

As today's threats are more—and in many ways different—than the traditional ones, security providers as well as the policies and mechanisms established to face those threats should be adjusted accordingly. Additionally, the increasingly globalized nature and interconnectedness of the international system, challenges state sovereignty and transnationalizes threats thus rendering the adoption of common (international) policies necessary. As Aravena puts it:

> coordinating policies, establishing regulations and generating international regimes based on shared values are essential points in designing a new international system for the twenty-first century. Only the ability to act jointly will enable states to recover their abilities to generate, together with other actors, a legitimate order capable of building a world free from threats and fear.[27]

It is true that such an approach is embedded in a neoliberal understanding of world politics and it could thus be criticized on many levels by advocates of different approaches. For example, given that most of the times security policies depend on who the security provider is, particular threats which are considered to be important to certain individuals, states, or non-state actors, might be given less attention than

---

[24] Barry Davies, *Terrorism*: *Inside a World Phenomenon* (London: Virgin Books, 2003). 253.

[25] Williams, "Security Studies: An Introduction," 9–10.

[26] Baldwin, "The Concept of Security," 16.

[27] Francisco R. Aravena, "Human Security: Emerging Concept of Security in the Twenty-First Century," *Human Security in Latin America* 2, no. 1 (2002): 7.

those actors would like if the only security agents were the international institutions. But in the case of a multileveled cybersecurity the logic regarding the security provider is different in that it is not limited to national or international policies of security management. Rather, the aim is to incorporate all concerned levels and actors into a common and collective multileveled framework, through which they would be able to produce multileveled, and globally oriented, policies of cybersecurity and cyber-defense. What are the implications of these conclusions for our definition of cyber-security and how could we go about establishing such a framework?

Cybersecurity has been defined as "a state's ability to protect itself and its institutions against threats, espionage, sabotage, crime and fraud, identity theft, and other precedents, and other destructive e-interactions and e-transactions."[28] Based on what we have examined so far and considering our aim of putting forward a multileveled cybersecurity, this definition seems rather narrow. In the context of this essay cybersecurity is the collective ability of individual, non-state, national, and international actors to protect each one of these levels against any type of disruptive or destructive cyberthreats, through a multileveled framework of cooperation, to the end of providing a secure and stable globally managed cyberspace. It is proposed that in order to accomplish the establishment of such a framework of multileveled cybersecurity, a certain security culture needs to be developed. The way in which we could develop a security culture that would correspond adequately to the challenge of such an understanding of cybersecurity is elaborated below.

13.3 International Cybersecurity Cooperation and Capabilities

Although the literature on international cooperation and institutionalism is extensive, there have not been made many concise efforts to approach international cooperation on cybersecurity. At the same time, whereas there is abundance of political and legal frameworks on perhaps every aspect of human life, the agreements and treaties with regard to cyberspace, and cybersecurity more specifically, are limited.[29] The few such treaties and agreements include the 2001 Convention on Cybercrime, by the Council of Europe, and the 2012 World Conference on Information Technology (WCIT-12). The latter was meant to revise the 1988 International Telecommunications Regulations treaty, and was led by the United Nations International Telecommunication Union (ITU).[30] Although WCIT-12 was an important step toward an international framework on cyberspace, the USA and other allies did not sign the final document over fears that governments would acquire control

[28] Choucri, *Cyberpolitics in International Relations*: 39.

[29] See, for example, Rex Hughes's call for a treaty on cyberspace, Rex Hughes, "A Treaty for Cyberspace," *international Affairs* 86, no. 2 (2010).

[30] Choucri, *Cyberpolitics in International Relations*: 168.

of the Internet. Eighty-nine other nations signed the final document[31] of the Conference but it has been argued that the refusal of many important Western states (e.g., the USA, Canada, and the UK) limit to a great extent the applicability of the agreed additions and revisions in the Convention of the ITU.[32]

Apart from international agreements and treaties, a number of various entities play a role in the "international institutional security ecosystem," at the international, national, and local level—including the private sector and nonprofit entities.[33] The North Atlantic Treaty Organization (NATO) and the European Union (EU) are two of the most important entities as they combine the local and regional levels while also having proceeded to the adoption of cybersecurity and cyber-defense policies.

NATO's commitment to the development of cyber-defense was evident as early as 2002 during the Prague Summit. Consequent Summits emphasized even more on the notion of a common cyber-defense while the new Strategic Concept of 2010 states that the Organization needs to have the necessary capabilities "to prevent, detect, defend against and recover from cyberattacks" as well as "enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations."[34] NATO's Cyber Defense Management Board, which has supplanted Cyber Defense Management Authority, makes a bold move toward bringing together key actors and centralizing the capabilities of the alliance with regard to cybersecurity and cyber-defense. At the same time, the Organization's cooperation with non-NATO nations in recent years has expanded its capabilities and cybersecurity management potentials.[35]

For its part, the EU has made its own efforts for the development of cybersecurity policies, most notably, by publishing its cybersecurity strategy, early in 2013. The five priorities of "Cyber Security of the European Union" are: the achievement of cyber resilience, the reduction of cybercrime, the development of a cyber-defense policy within the framework of the Common Security and Defense Policy (CSDP),

---

[31] ITU, *Final Acts*: *World Conference on International Communication* (Dubai: International Telecommunications Union, 2012).

[32] Cyrus Farivar, "The UN's telecom conference is finally over. Who Won? Nobody Knows.," ars technica, http://arstechnica.com/tech-policy/2012/12/the-uns-telecom-conference-is-finally-over-who-won-nobody-knows/.

[33] See a list of major entities at all these levels in, Choucri, *Cyberpolitics in International Relations*: 161–66.

[34] NATO, *Active Engagement*, *Modern Defence. Strategic Concept for the Defence and Security of the Members of th North Atlantic Treaty Organization* (Lisbon: NATO, 2010). 16–17; Marios P. Efthymiopoulos, "NATO's Security Operations in Electronic Warfare: the Policy of Cyber-Defence and the Alliance's new Strategic Concept," *Journal of Information Warfare* 8, no. 3 (2009): 64–66.

[35] Victoria Ekstedt, Tom Parkhouse, and Dave Clemente, "Commitments, Mechanisms & Governance," in *National Cyber Security*: *Framework Manual*, ed. Alexander Klimburg (Tallinn: NATO CCD COE Publication, 2012), 185; Jason Healey and Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," *Atlantic Council* IssueBrief(2011): 4.

the development of "industrial and technological resources for cyber security," and the establishment of "a coherent international cyberspace policy" for the Union.[36] These strategic priorities are also based on a number of principles; yet two of those principles stand out as they are particularly important for the future of cybersecurity as put forward in this essay: (1) "Democratic and efficient multi-stakeholder governance," and (2) "A shared responsibility to ensure security." The former acknowledges the importance of multiple stakeholders—e.g., commercial, nongovernmental, and governmental entities—and supports their role in a "multi-stakeholder governance approach" for the EU, while the latter calls for "shared responsibility" and "coordinated response" by all relevant actors, at all levels, for a stronger cybersecurity.[37]

The examples of both the EU and NATO demonstrate recent, yet significant, efforts toward a coherent and broader cybersecurity framework. Even more essential for the accomplishment of this end seem to be the established and developing frameworks of cooperation between the EU and NATO. The two Organizations have been cooperating closely particularly since 2003 within the framework of the "Berlin Plus" agreement, while NATO has been also cooperating with the European Defense Agency (EDA), which has prioritized cyber-defense. Despite a number of existing agreements that regulate the NATO–EU cyber cooperation, there are still problems with its expansion to other sectors due to data protection concerns, the different perceptions of EU non-NATO states, as well as different perceptions between the two Organizations.[38]

The disagreements—no matter how minor—between two Organizations with such a similar security culture—given the big overlap with regard to their members—and history of cooperation, brings us to a common problem in international relations and politics, the one of conflicting (national) interests. Deibert and Rohonzinski, while acknowledging the growing international consensus on cybersecurity, they argue that this is not always the case, especially "when it comes to risks *through* cyberspace." In specific, they maintain that, "While states do collaborate around some policy areas where consensus and mutual interests can be found (for example, 'piracy,' and to a lesser degree child pornography), cooperation declines as the object of risk becomes politically contestable and where national interests can vary widely."[39] This, in turn, brings us to the realization that as long as individual nations have their own interests and maintain their own offensive and defensive (cyber) capabilities, full cooperation with regard to cybersecurity can only be limited. After all there have been many incidents over the past decade of cyberattacks from one

[36] EU, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," JOIN(2013) 1 final(07/02/2013): 4–5.

[37] Ibid., 3–4.

[38] Ekstedt, Parkhouse, and Clemente, "Commitments, Mechanisms & Governance," 186–87.

[39] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4(2010): 17.

country to another, such as China's attacks against the USA.[40] In this light, a need emerges for finding the ways in which the international community and global civil society could join forces in establishing a multileveled management of cybersecurity. One such way could be the development of a security culture that would foster multileveled cooperation on cybersecurity.

13.4 Security Culture and Global Capacity Building

Security culture has been related, among others, to organizational and (national) strategic culture and it is in many ways based on cognitive psychology and ideational understandings of security. In this essay we draw upon strategic culture definitions to shape our own definition of cybersecurity culture in the context that has been analyzed above.[41]

Jack Snyder was the first to examine the concept of strategic culture which he defined as "the body of attitudes and beliefs that guides and circumscribes thought on strategic questions, influences the way strategic issues are formulated, and sets the vocabulary and the perceptual parameters of strategic debate."[42] Kupchan's narrower view focuses on how elites make strategic decisions, and argues that "deeply embedded conceptions of security and notions of empire take root among elites and masses alike" while stressing that "strategic culture is distinguishable from elite beliefs [because]…it is based on images and symbols, not on logic and causal inference."[43] Johnston also emphasizes the importance of "symbols" while he maintains that two basic elements constitute strategic culture: "a central paradigm" which has answers regarding symbols, like "the nature of conflict in human affairs, the nature of the enemy, and the efficacy of violence; and "a ranked set of strategic preferences logically derived from these central assumptions."[44]

Even broader are the definitions by Booth and Gray. Booth suggests that "strategic culture refers to a nation's traditions, values, attitudes, patterns of behaviour, habits, customs, achievement and particular ways of adapting to the environment and solving problems with respect to the threat or use of force."[45] A similar, though shorter, definition is the one by Gray: "Strategic culture is the world of mind, feeling,

[40] Nigel Inkster, "China in Cyberspace," *Survival*: *Global Politics and Strategy* 52, no. 4 (2010): 55–56.

[41] Alexander W. Vacca, "Military Culture and Cyber Security," *Survival* 56, no. 6 (2012): 160.

[42] Jack L. Snyder, *The Strategic Culture*: *Implications for Nuclear Options* (Santa Monica: RAND, 1977). 9.

[43] Charles A. Kupchan, *The Vulnerability Of Empire* (New York: Cornell University Press, 1994). 21–22.

[44] Alastair I. Johnston, *Cultural Realism*: *Strategic Culture and Grand Strategy in Chinese History* (New Jersey: Princeton University Press, 1995). 50–51, viiii-x.

[45] Ken Booth, "The Concept of Strategic Culture Affirmed," in *Strategic Power*: *USA*/*USSR*, ed. Carl G. Jacobsen (New York: St. Martin's Press, 1990), 121.

and habit in behavior."[46] In this context, ideas matter and should be taken into account when examining or developing policies as well as when we try to develop frameworks of cooperation. As the above definitions show, strategic culture explanations mostly concern the national level and the distinct characteristics that shape the ways nations act on or react to strategic and security matters. Yet strategic culture has also been used to refer to different levels such as the military level or even the international level, i.e., strategic culture of a collective security organization. With regard to cybersecurity Paul and Porche III define an Army cybersecurity culture as "A pattern of shared basic assumptions that supports information security becoming a natural aspect of the daily activities of all Army personnel who operate in cyberspace."[47]

The security culture that this essay suggest is much broader and even though it goes beyond national strategic cultures, it does not disregard their existence; contrarily, it takes the variety of strategic cultures seriously into account as that is the only way the appropriate common features could be identified for the development of a new, collective, security culture of multileveled cybersecurity. After all, it has been argued that strategic culture could also be applied to non-state or transnational actors like the EU.[48] In this instance we refer to a culture of security instead of strategy as what we do not want to trace the ideas and norms that shape the strategic behavior of an actor but rather find ways to socialize different (national) ideas and norms—whatever they may be—into a global security culture of cybersecurity. A cybersecurity strategy therefore is the outcome we are interested in, not our object of analysis; but for such a strategy to be adopted a security culture needs to be developed first. Drawing upon the above-mentioned definitions, a security culture of multileveled cybersecurity would be a body of collective—i.e., non-state, sub-national, and national—attitudes, patterns of behavior, beliefs, as well as conceptions of (cyber) security, shaped based on the need to secure multiple referent objects against various cyberthreats, which would influence cybersecurity strategies.

It has been argued before that institutions have the power to shape common ideas and interests. As far as cybersecurity is concerned we do agree with the view that "institutions may well be the precursors for formalizing norms and principles that, in turn, might consolidate and strengthen the institutions themselves."[49] But because, as we have shown, many issues are subjects to political contestation among nations, the starting point of cooperation should be one that is valued by all actors involved. For example, it would be fairly difficult to integrate multiple national or military security cultures within a broader security culture framework. That is also the case

[46] Colin S. Gray, "Strategic Culture as Context: The First Generation of Theory Strikes Back," *Review of International Studies* 25(1999): 58.

[47] Christopher Paul and Isaac R. Porche III, "Toward a U.S. Army Cyber Security Culture," *International Journal of Cyber Warfare & Terrorism* 1, no. 3 (2012): 71.

[48] Perm M. Norheim-Martinsen, "EU Strategic Culture: When the Means Becomes the End," *Contemporary Security Policy* 32, no. 3 (2011): 535.

[49] Jeremy Ferwerda, Nazli Choucri, and Stuart Madnick, "Institutional Foundations for Cyber Security: Current Responses and New Challenges (revised)," *Composite Information Systems Laboratory*, *MIT* Working Paper CISL# 2011-05(2011): 4.

Table 13.1 Recent cyberthreat perceptions and cyberattacks

Actors	Incidents	Month/year	Type
Iran against West	Iran carries out cyber-drills	December, 2012	State vs. State (*Political*)
China against USA	USA asks China to halt corporate cyberattacks	February, 2013	State vs. State/Corporations (*Commercial*)
"Anonymous" against Governments, e.g., Israel	"Anonymous" launch attack on Israel	April, 2013	Transnational entity vs. states/governments (*Political*)
Anti-Western hackers (Syria) against West	Syria-based pro-Assad hackers (Syrian Electronic Army) attack Western media	April, 2013	Non-state/individual actors vs. non-state Organizations (*Political*)
Anti-Western hackers (Iran) against USA	Iranian-based hackers attack US company	May, 2013	State vs. State (*Political*)
China against USA	USA accuses China of cyber-spying	May, 2013	State vs. State (*Political*)

with cybersecurity as each nation—especially great powers—have related their cybersecurity and cyber-defense with their military and national strategies. The domain of cyberspace is, arguably, much more important than any other domain of international cooperation because of the multiple referent objects to be secured and the global implications of cyberthreats, as analyzed above. This reality—if we may call it that—could constitute the perfect starting point for cooperation on cybersecurity and the eventual development of a corresponding security culture.

In order for that to be achieved, two parallel tactics should be considered/undertaken: cooperation on all and through levels (horizontal and vertical cooperation); and cooperation on common cybersecurity threats—i.e., shared threats, common individual threats, and threats with potentially global impact. Starting with the latter we need to identify some serious cyberthreats with global or international concern. Table 13.1 briefly articulates a few cyberthreat perceptions or actual cyberattacks of different kinds in recent of years. It is important to note that threat perceptions do matter as they influence policy-making. By looking at the table one can identify the different types of cyberthreats, the different actors involved and, therefore, the multiple referent objects that need to be secured. It is important to note that the table is by no means exhaustive.

It is clear that there are differences between states which are expressed in cyberspace as well. Most notable cyber rivalries—at least as far as the table is concerned—are between the USA and China, the USA and Iran, and Israel and Iran. Cyberattacks were also carried against Iran from the USA and Israel in 2009.[50] From that perspective, cooperation could not be initiated based on politically sensitive issues like the cybersecurity of Iran's nuclear program, or the US government

[50] Shaun Waterman, "U.S.-Israeli Cyberattack on Iran was 'Act of Force,' NATO Study Found," The Washington Times, http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all.

cybersecurity vis-à-vis Chinese cyberthreats. The best starting point for multi-leveled and international cooperation on cybersecurity would be the common threats that all levels and governments face from individuals, non-state, and transnational actors—provided that they do not have state-sponsored political aims. Then more important issues could be gradually added to the agenda.

A multileveled cooperation and security culture could only be developed if efforts were made to bring together different actors on each level as well as built efficient communication lines between levels. As such, the sought collective cybersecurity culture would be informed by all levels through a top-down/bottom-up approach with no imposition of rules, regulations, or policies by one level on another. On a sub-national level, non-state actors such as banks, different firms, multinational companies and corporations, transportation and communication companies, would be easier to collaborate rather than governments. Therefore, existing domestic, regional, and international frameworks of cooperation need to be further developed in order for a global network to be created; a network, which would deal with—mainly commercial–cybersecurity concerns of private non-state entities. Such concerns could be cyber disruptions as well as data or intelligence theft by individuals or other private entities.

On a national level states should develop—as many have already done—their own cyber-defense not only for military purposes but for the security of their administrative (cyber) infrastructures as well. However, the know-how of each state should be shared as much as possible with other states, within the framework of global cooperation. Regional organizations could play an instrumental role to that end. Entities such as NATO, the EU, the Organization for Security and Cooperation for Europe (OSCE), the Association for Southeast Asia Nations (ASEAN), the African Union (AU), and the Union of South American Nations, among others, could facilitate an international dialogue on cybersecurity at the regional level as a first step. Understandably some of these institutions are more focused on trade and economic cooperation; yet a focus on cybersecurity would be an opportunity for further integration. In the meantime, at the national level, non-state actors should be in coordination both with the government and with the relevant regional institution.

The key for a global integration of different entities and different cybersecurity concerns is interregional/organizational dialogue. That would be the last step for the completion of the multileveled and globally oriented scheme of cooperation (see Fig. 13.1 for a depiction of the proposed framework). In sum, horizontally, non-state actors based in different states should cooperate among them, states should also cooperate on a (bilateral or multilateral) government level, states should participate in international institutions of their region, and regional institutions should participate in interregional coordination. Vertically, all levels should maintain effective communication lines and coordination between them. The non-state level should communicate with the state and regional level and vice versa, the state level should communicate with the non-state level as well as with the regional institutional level and vice versa, while the regional institutional level should coordinate with other regional institutions at the interregional—and ultimately global—level. Further, in terms of the agenda, the issues to be addressed and dealt with should be

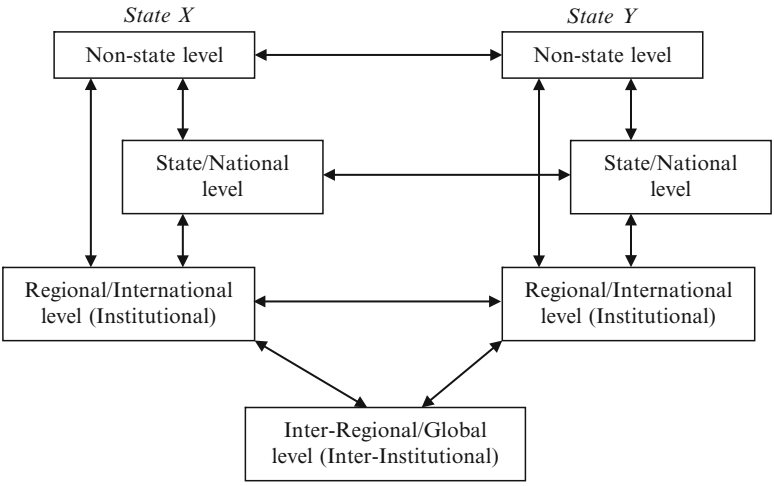

Fig. 13.1 Multileveled cybersecurity cooperation

gradually more important and politically sensitive. Cooperation should start from commercial, everyday life, and notably non-state, matters only to gradually proceed to national, governmental and military issues. Thereby, the development of a global security culture of multileveled cybersecurity would be more possible and with greater potentials not only for cybersecurity but for international peace as well.

13.5 Conclusions

This essay has demonstrated the impact of cyberspace in everyday life and therefore the great insecurity that stems from cyberthreats at all levels—the local, national, and international. Against this background, and given that cybersecurity is in every actor's interest, there has been suggested that in order for global and effective cybersecurity and defense to exist a security culture of cybersecurity should be gradually developed through horizontal and vertical multileveled cooperation by starting with "low-politics" or non-politically sensitive cybersecurity matters. We have accepted that there may be many reasons for states not to cooperate, and states may indeed be the actors which would pose the biggest challenge in the context of a multileveled cybersecurity. However, cyberspace might be the one thing with the potential of effectively going beyond the notion of state-centric power struggle and that is because of its increasing and essential role in interconnecting all kinds of interests of all kinds of actors within the global system. In fact, we could go so far as to suggest that a multileveled framework of cybersecurity with successful communication lines through and between all levels may even provide a good platform for cooperation in other domains as well—through the socialization of norms and ideas—thus marking the beginning of further integration and interconnectedness of interests.

Yet this idea needs to be further developed and researched based on the already existing frameworks of cooperation at all levels in order for specific guidelines to be suggested and ways through which these frameworks could be integrated to be found.

Bibliography

Aravena FR (2002) Human Security: Emerging concept of security in the twenty-first century. Human Security in Latin America 2(1):5–15

Baldwin DA (1997) The concept of security. Rev Int Studies 23:5–26

Booth K (1990) The concept of strategic culture affirmed. In: Jacobsen CG (ed) Strategic power: USA/Ussr. St. Martin's Press, New York, NY, pp 121–128

Booth K (1991) Security and emancipation. Rev Int Studies 17(4):313–326

Buzan B, Hansen L (2010) The evolution of international security studies. Cambridge University Press, Cambridge

Choucri N (2012) Cyberpolitics in international relations. MIT, Cambridge

Davies B (2003) Terrorism: Inside a world phenomenon. Virgin Books, London

Deibert RJ, Rohozinski R (2010) Risking security: Policies and paradoxes of cyberspace security. Int Polit Sociol 4:15–32

EC (2005) Green Paper: On a European Programme for Critical Infrastructure Protection. Commission of the European Communities COM(2005) 576

Efthymiopoulos MP (2009) Nato's security operations in electronic warfare: The policy of cyber-defence and the alliance's new strategic concept. J Inform Warfare 8(3):61–70

Ekstedt V, Parkhouse T, Clemente D (2012) Commitments, mechanisms & governance. In: Klimburg A (ed) National cyber security: Framework manual. NATO CCD COE Publication, Tallinn, pp 146–191

EU (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final (07/02/2013)

Farivar C (2012) The Un's Telecom Conference Is Finally Over. Who Won? Nobody Knows.ars technica,http://arstechnica.com/tech-policy/2012/12/the-uns-telecom-conference-is-finally-over-who-won-nobody-knows/

Ferwerda J, Nazli C, Stuart M (2011) "Institutional Foundations for Cyber Security: Current Responses and New Challenges (Revised)." Composite Information Systems Laboratory, MIT Working Paper CISL# 2011–05, http://web.mit.edu/smadnick/www/wp/2011-05.pdf.30/04/2013

Giddens A (1990) The consequences of modernity. Polity, Cambridge

Gray CS (1999) Strategic culture as context: The first generation of theory strikes back. Rev Int Studies 25:49–69

Healey J, van Bochoven, L (2011) Nato's Cyber Capabilities: Yesterday, Today, and Tomorrow. Atlantic Council IssueBrief

Hughes R (2010) A treaty for cyberspace. Int Affairs 86(2):523–541

Inkster N (2010) China in cyberspace. Survival: Global Politics and Strategy 52(4):55–66

ITU (2012) Final Acts: World Conference on International Communication. International Telecommunications Union, Dubai

Johnston AI (1995) Cultural realism: Strategic culture and grand strategy in Chinese history. Princeton University Press, Princeton, NJ

Kupchan CA (1994) The vulnerability of empire. Cornell University Press, New York, NY

McSweeney B (1999) Security, identity and interests: A sociology of international relations. Cambridge University Press, Cambridge

NATO (2010) Active engagement, modern defence. Strategic concept for the defence and security of the members of the North Atlantic Treaty Organization. NATO, Lisbon

Norheim-Martinsen PM (2011) Eu strategic culture: When the means becomes the end. Contemporary Security Policy 32(3):524–541

North RC (1990) War, peace, survival: Global politics and conceptual synthesis. Westview Press, Boulder, CO
Nye JS (2011) The future of power. Public Affairs, New York, NY
Panyarachun A et al (2004) A More secure world: Our shared responsibility. High-level panel on threats, challenges and change: United Nations, Manhattan
Paul C, Porche IR III (2012) Toward a U.S. Army cyber security culture. Int J Cyber Warfare Terrorism 1(3):70–80
Prezelj I (2008) Challenges in conceptualizing and providing human security. HUMSEC J 2:1–22
Rosenfield DK (2009) Rethinking cyber war. Crit Rev 21(1):77–90
Snyder JL (1977) The strategic culture: Implications for nuclear options. RAND, Santa Monica
Terriff T et al (2006) Security studies today. Polity, Cambridge
Ullman RH (1983) Redefining security. Int Security 8(1):129–153
Vacca AW (2012) Military culture and cyber security. Survival 56(6):159–176
Walt SM (1991) The renaissance of security studies. Int Studies Quarterly 35(2):211–239
Waterman S. U.S.-Israeli Cyberattack on Iran Was 'Act of Force,' Nato Study Found. The Washington Times, http://www.washingtontimes.com/news/2013/mar/24/us-israeli-cyberattack-on-iran-was-act-of-force-na/?page=all
Williams PD, Studies S (2010) An Introduction. In: Williams PD (ed) Security studies: An introduction. Routledge, New York, NY, pp 1–10
Wolfers A (1952) 'National security' as an ambiguous symbol. Polit Sci Quarterly 67(4):481–502

Chapter 14
The Relevance of Endpoint Security in Enterprise Networks

Ian Ahl

Abstract The amount of and sophistication of cyberattacks continue to grow at a feverish pace. There was a time when having AntiVirus deployed was the extent of an Endpoint Security solution, but that is no longer the case. Organizations must consider a more comprehensive Endpoint Security approach to complement other security controls applied at the network and application levels. While Endpoint Security is somewhat complex, once deployed and tuned the rewards can be great.

Keywords Endpoint security • Malware • Firewall • Intrusion prevention system • Architecture

14.1 Introduction

Symantec reports that in 2011 they detected and stopped more than 5.5 billion malicious attacks, which was an increase of over 80 % from 2010.[1] As this statistic is only from a single vendor, it is reasonable to believe that the actual number of attacks is substantially higher, especially considering that many attacks go unnoticed. These statistics differ based on the organizations that are reporting them, but the main theme is clear—there are a myriad of attacks, and their number grows exponentially year by year. Governments and commercial organizations are becoming increasingly more proactive and prepared to defend their assets against attackers. A prime example of this is the United States Department of Defense (DoD) Host Based System Security (HBSS) program that focuses on the implementation

[1] http://www.symantec.com/about/news/release/article.jsp?prid=20120429_01

I. Ahl (✉)
FireEye, Inc., Milpitas, CA, USA
e-mail: ian.ahl@tekdefense.com

E.G. Carayannis et al. (eds.), *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*,
DOI 10.1007/978-1-4939-1028-1_14,

and configuration of endpoint security products. While many organizations have focused on securing their network perimeters, the DoD is shifting focus to the security of their hosts. Endpoint Security is an essential and often underdeveloped layer in the Defense in Depth (DiD) model. Endpoint Security is in many ways more complex to maintain than boundary security mechanisms, but once properly configured, the results are rewarding.

14.2 What Is an Endpoint?

In the age of Bring Your Own Device (BYOD), the definition of an "Endpoint" is evolving quickly. In many organizations, endpoints are servers and Microsoft PCs, while in others there are Apple components, tablets, Point of Sale (POS) terminals and other network attached devices. Some may consider VoIP Phones, Blackberry devices, smart phones, printers and other devices as endpoints as well. In this chapter we will focus on traditional endpoint devices such as servers and workstations, although the principles and methodologies discussed also apply to any network connected computing devices.

14.3 General Challenges

Within this chapter, we will explore the challenges that are unique to each of the different Endpoint Security modules. However, before diving into those, it is important to first understand the general challenges that affect all Endpoint Security modules.

14.3.1 Not Just AV

When most people hear "Endpoint Security" they immediately think of AntiVirus (AV). Many do not understand that there is more to Endpoint Security than classic signature based AV. While AV may be the most popular Endpoint Security product, the argument could be made that it is the least effective of all the Endpoint Security technologies. Technologies like host based firewalls, intrusion prevention systems, data loss prevention, rogue host detection, device control, and application whitelisting are vital to the success of an Endpoint Security program.

14.3.2 "No Man Left Behind"

One of the greatest challenges associated with endpoint security is the sheer volume of endpoints an organization has to protect. Unlike boundary security, where organizations can focus security efforts on key network locations, Endpoint Security

must consider each separate component. A single compromised host can lead to a significant infection, data breach, or other attack. As any host can be a pivot-point that provides access to other hosts on a network, endpoint devices must be protected at all times. For most Endpoint Security solutions this means that all hosts must have the security products installed, configured and running consistently and constantly. This can be an insurmountable task for any organization to implement, deploy, maintain, monitor, and respond.

To put this into perspective, let's consider patch management, which should be easy now that everyone has had years of practice, right? Unfortunately, there are not many organizations that can even say that every Microsoft Windows machine is fully patched, much less the non-Microsoft based systems. It is often hard for senior leadership to accept that 100 % patch compliance is not obtainable due to incompatibility issues.

This issue is similar in the case of Endpoint Security. There will always be a machine that is not compatible with the selected Endpoint Security software due to unsupported or legacy applications or Operating Systems. Other issues may include problems resulting from software crashes, misconfigurations, and other software problems. These conditions require organizations to actively monitor for hosts that do not meet the established criteria for Endpoint Security and remediate them. Notwithstanding, in later sections, there are many tools in the endpoint security arsenal that help limit the effect that a compromised host can have on an organization.

14.3.3 Complexity

Another traditional problem that plagues Endpoint Security is the complexity of the standard solutions. It is relatively simple for even non-technical folks to understand the concepts behind a network firewall, proxy, or even an Intrusion Detection System (IDS). For Security Engineers, network security products like those just named are well understood and have years of best practices and guidelines to support their implementation and operation.

Endpoint Security solutions are much more complex, and have not been around long enough for security engineers to have built up a robust set of best practices. One example of this complexity is application whitelisting. In order to implement an application whitelisting solution, engineers must fully understand all applications and their dependencies, while also understanding application hooking, hashing, and other detailed technologies. Thus, the configuration can be quite complex.

Likewise, complexity may show up in other areas, such as deployment and architecture. For instance, organizations need to understand the effect Endpoint Security products may have on the resources of the host, and the network itself. If an Endpoint Security product is configured to send all events to a central server across the network, the connection can cause network saturation, and in some cases, a significant operational impact.

14.3.4 Standardization

In order to properly deploy a full Endpoint Security solution, an organization must first have a firm understanding of their hosts and their network. Going beyond what Operating Systems (OS) are installed, an organization must also know what applications are installed, what network communication is expected, the type of data on the machine, and the general purpose of the device, among other details. Essentially, an organization must have an extensive baseline for their devices. Starting the deployment of each system from a standard build and following predefined configuration guidelines can help an organization with building their baseline. This is a concept that will be explored in greater detail in the application whitelisting section. To help maintain standardization after systems are deployed, organizations must also utilize a well-defined configuration and change management plan. The Change Control Board (CCB) should include security engineers that can gauge the impact a change may have on Endpoint Security.

14.3.5 Configuration Matters

Most Endpoint Security suites have only a subset of features enabled by default. This is often done to address consumer concerns with functionality, complexity and operational impact. If an organization leaves Endpoint Security products installed with default configurations, the full potential of the products will most likely not be reached. Endpoint Security must be tailored to each organization's needs. Rather than disregard these choices because they are too difficult, organizations should conduct an assessment to determine which features provide the most value for their environment. A recent example comes from the very public NY Times hack reported in January, 2013.

The Register reported[2]:

Quote from NY Times:

> Over the course of 3 months, attackers installed 45 pieces of custom malware. The Times — which uses antivirus products made by Symantec — found only one instance in which Symantec identified an attacker's software as malicious and quarantined it, according to Mandiant.

Symantec's Response:

> Advanced attacks like the ones the New York Times described … underscore how important it is for companies, countries and consumers to make sure they are using the full capability of security solutions. The advanced capabilities in our endpoint offerings, including our unique reputation-based technology and behaviour-based blocking, specifically target sophisticated attacks. Turning on only the signature-based anti-virus components of endpoint solutions alone are not enough in a world that is changing daily from attacks and threats. We encourage customers to be very aggressive in deploying solutions that offer a combined approach to security. Anti-virus software alone is not enough.

[2] http://www.theregister.co.uk/2013/02/01/symantec_responds_nyt_apt/

Based on this response, it appears that Symantec believes the attacks would have been more likely detected and stopped if the NY Times had utilized the full capabilities of the Endpoint Security suite.

14.4 Endpoint Security Architecture

When choosing and deploying an Endpoint Security solution for an enterprise, a critical element is the architecture. Will there be central management? Will there be central logging? How will endpoints receive the initial product installation files and subsequent updates? What impact will the Endpoint Security solution have on the hosts themselves? Which groups will manage analysis, maintenance, troubleshooting, configuration, etc.? How much bandwidth is available? What traffic load can be expected from the Endpoint Security products at particular times during the day? These are just some of the questions organizations need to ask themselves when considering how to employ their Endpoint Security solution.

14.4.1 Deployment Considerations

14.4.1.1 Centralized vs. Decentralized Management

When deploying an Endpoint Security suite, one of the first items an enterprise must consider is how the product will be managed. To better illustrate, let's create a company called XYZ corp. XYZ corp. is a large enterprise with global offices. They have a central Network and Security Operations Center (NSOC) in Washington DC, and regionalized NSOCs in locations such as Germany, California, Japan, and Australia. Overall they have 350,000 endpoints (servers and workstations). XYZ corp. has the following choices they could make on the management aspect:

- Fully Centralized: In a fully centralized approach, XYZ corp. would manage all devices from their DC NSOC. No activity would be delegated to the regional offices, although the regional offices would most likely be informed of the activities via a change or configuration management process.
- Centralized with regional responsibilities: Utilizing a centralized approach with regional delegation, the central NSOC dictates base configurations, performs logging, and maintains the supporting infrastructure, while also verifying that regional tasks are being completed. The regions are responsible for implementing the base configurations. They can make configurations tighter but cannot implement less restrictive configurations without approval from the central NSOC.
- Decentralized: Each region is completely responsible for its own Endpoint Security solution. There may not be oversight or a central authority dictating policy or standards, and analysis of logs is managed within each region.

There are advantages and disadvantages to each of these approaches. Organizations must fully understand the risks associated with each deployment type and the impact to the organization. Generally speaking, most organizations end up deciding to implement the hybrid approach of a centralized entity for oversight and monitoring and delegated responsibilities to subordinate locations.

14.4.1.2 Organizational Structure

Regardless of which Management approach is selected, organizations also need to consider how the different core responsibilities of Endpoint Security will be organized. For instance, will an enterprise have a single team responsible for all Endpoint Security related activities or will responsibilities be split up and handled by multiple teams. Like other security products, Endpoint Security roles can be divided into functional groups. These functional groups may include:

- Maintenance: Responsible for the health of the databases, servers, and other dependent devices that make up the Endpoint Security architecture.
- Help desk: Responsible for fielding customer calls on issues related to the Endpoint Security products. There may be several tiers of support in this group.
- Analysis: Responsible for monitoring events and logs from the Endpoint Security solution for incidents.
- Signature development: Responsible for creating signatures to block or monitor specific activity the organization would like to target.

Some organizations may include other functional groups as well. The main decision point is how to organize these functional groups. This decision will depend on factors such as the number of members of the Endpoint Security team, the number of assets being protected, the sensitivity of the data being protected, the existing security structure, and the geographical range of the organization. Organizations must take all of these factors into consideration when deciding how to structure the support team(s).

14.4.2 Host Resources

Ironically, one of the items often not considered when deploying an Endpoint Security Solution is the host itself. There are three main considerations involving the host: resource consumption, compatibility, and application specific configurations.

14.4.2.1 Resource Consumption

The entire suite of tools in an Endpoint Security solution can have a significant impact on a host's resources (CPU, memory, and network bandwidth). While the resource-draw will be heavily dependent on the configuration of the Endpoint Security

solution, there is often a noticeable impact for at least some of an enterprise's user base, which inevitably leads to a tarnishing of the reputation of the Endpoint Security solution. Further, the implementation almost always becomes the scapegoat for many "My computer is acting slowly" complaints and leads to users attempting to circumvent the security software to improve performance. While this cannot be entirely avoided, the following steps can help mitigate performance issues:

- Thoroughly test and evaluate Endpoint Security solutions to find the appropriate product that fits the needs of the organization.
- Upgrade hardware on the host devices when required.
- Pay attention to configuration items that can impact resource consumption.

The configuration items that can impact resources will vary based on the Endpoint Security solution utilized and the applications on the host.

14.4.2.2 Compatibility

Not all Endpoint Security solutions are compatible with all hardware, operating systems and applications. Organizations must closely consider which Endpoint Security solution to utilize based on the devices and applications they intend to protect. For instance, if an organization relies mostly on Windows 2000, then it would not want McAfee CMA 4.5 or greater.[3]

14.4.2.3 Application Specific Configurations

There are many applications on a host that require specific configurations within Endpoint Security products to ensure functionality is not broken and host resources are not adversely affected. For instance, scanning the transaction log of a database with an AV program can often cause database corruption and excessive resource utilization. To avoid such issues, administrators of the Endpoint Security solution should work with system and application administrators to identify any special configurations that need to be considered. To accommodate this, it is often recommended to create core configurations for operating systems and major applications in use. For instance, an administrator may consider creating policies for each of the following:

- Windows XP
- Windows 7
- Windows Server 2008
  - Active Directory
  - SQL
  - IIS

[3] https://kc.mcafee.com/corporate/index?page=content&id=KB51573

- Linux
  - Apache
  - MySQL

As this chapter progresses the reader will see how structuring policies and configurations in this fashion can prove very useful for an organization.

14.5 Endpoint Security Technologies

Endpoint Security technologies have grown substantially in the past 10 years. While AV has been around for a long while, it was not until recently that other host based security solutions, such as host based firewalls, Intrusion Prevention Systems, and data loss prevention techniques, have become available. These technologies are often overlooked and misconfigured, but once configured and deployed properly, they can become the most useful detection and blocking technologies available. A robust Endpoint Security solution will encompass a variety of protective measures.

14.5.1 Management/Analysis Server

The foundation of an effective Endpoint Security solution is the central management and analysis device. Endpoint Security technologies are complex. The mission of the central management server is to alleviate the complexities by providing administrators with a single console to configure policies for Endpoint Security products. Consider again XYZ Corporation with their 350,000 endpoints. Without a central management platform, would it be feasible for XYZ corp. to install, configure, maintain, and monitor Endpoint Security products on each endpoint? While possible, it would be a very ineffective deployment method. McAfee's platform for this is the ePolicy Orchestrator (ePO) server. Using a central server like this, an organization can administer Endpoint clients in the same method that they manage their Active Directory hierarchical structure. For instance, with ePO, an organization can create a structure such as the following:

1. Central NSOC
   (a) Region1
       - Windows Servers
         - Active Directory
         - SQL
         - IIS

- Linux Servers
  - Apache
  - MySQL
- Workstations
  - XP
  - Win7

(b) Region2

- Windows Servers
  - Active Directory
  - SQL
  - IIS
- Linux Servers
  - Apache
  - MySQL
- Workstations
  - XP
  - Win7

(c) Region3

- Windows Servers
  - Active Directory
  - SQL
  - IIS
- Linux Servers
  - Apache
  - MySQL
- Workstations
  - XP
  - Win7

With this structure, an administrator can assign policies, run reports, or give permissions at each separate level. While this is a somewhat simple structure, an organization can expand this concept to fit their unique situation.

In an enterprise environment, all events and logs from endpoint solutions should be sent to a Security Information and Event Management (SIEM) solution but should also be available via a central analysis platform native to the Endpoint Security solution. McAfee handles this with their ePO server, while some other vendors separate analysis from the management server. Utilizing this analysis platform, a security

analyst will be more capable of performing investigations on suspicious host based indicators. While we do not focus on event analysis, it is important to realize that this is a facet of the Endpoint Security solution.

14.5.2 AntiVirus/AntiSpyware

The first products most people think of when considering Endpoint Security are AV and AntiSpyware (AS). While these are the traditional Endpoint Security products, they are often widely considered the least effective.[4] To put this in perspective, readers must understand what AV products have to contend with. There are literally millions of pieces of malware.[5] Most signatures are written specifically for a single malware sample. Even with automated systems it is no easy task for these products to keep up with the onslaught of attacks, thus leading to low detection rates across the board. For example, to circumvent AV, simply create a new piece of malware or use a method like packing or obfuscation to make the malware appear unique.

This is not to say that removing AV is the correct answer. AV provides a needed service within the DiD structure, and it still provides a great solution for the low hanging fruit. AV vendors have realized the problem with the signature-based approach for many years and have attempted to defeat this by using heuristics engines. Rather than looking for a specific file, driver, or string the way signature based detection does, heuristics watch for "behaviors" of malware. These behaviors can be items like modifying certain files, creating a process, making a connection, injecting a process, etc. Heuristics engines are not typically enabled by default. Heuristics engines are often blamed for false positives and resource utilization, although currently there is not much data to refute or confirm those claims. Be sure to test this feature in your environment before deploying it.

AV, like any other product, can cause severe issues when not configured properly. One configuration option that an enterprise should be aware of is the ability to place exclusions on certain files or directories from scanning. When deploying AV across an enterprise, the Endpoint Security administrators need to hold discussions with application and systems administrators to determine which application files should be excluded from scans. Most vendors of commercial applications provided a documented list of files that should be excluded from scans. Microsoft does a particularly good job at this.[6] Keep in mind that attackers know that exclusions may be in place, and will attempt to leverage this as well. To combat this, be as specific as possible with exclusions. For instance, rather than excluding all files with an extension of .mdb, include the path in the exclusions—for example, *d*:*database***.mdb*.

[4] http://www.techrepublic.com/blog/security/new-controversy-on-the-effectiveness-of-antivirus-software/8919

[5] http://www.cso.com.au/article/419622/how_much_malware_has_arrived_since_1984_/

[6] http://support.microsoft.com/kb/822158

14.5.3 Host Based Firewall

Many security engineers believe the boundary firewall to be the one security device that they cannot live without. Firewalls, in general are packet filtering or stateful inspection devices. Host based firewalls (HBFW) bring the power of a firewall onto every host, thus combining boundary-type security with application specific controls. There are some features that make host based firewalls much more capable than a traditional network firewall—application awareness, connection aware groups, hash matching, etc. Thus, a well-configured host based firewall may prove to be the most valuable Endpoint Security product for many organizations.

A traditional network based firewall can filter traffic based on the source, destination, and port. Next Generation network firewalls are now introducing filtering based on the application layer as well, but this functionality is still very limited because the firewalls rely heavily on traffic not being encrypted and on having a signature for the application's traffic pattern. To truly understand what data the firewall is seeing, a signature would need to be created for every application that communicates over the network.

HBFWs on the other hand don't run into these issues. Most HBFWs can filter traffic based on source, destination, port, and application. Sounds the same as a network firewall, right? On the surface it is, but a closer look reveals that the main difference is in the application communication filtering. For a HBFW, the host knows that iexplorer.exe is attempting to initiate and outbound connection. It doesn't need to match the network traffic up to a signature to determine this. Thus, it can make a quicker and hopefully, more accurate determination as to whether the traffic is legitimate or not.

The value of the HBFW is largely based on how it is configured. Within the DiD model, organizations should configure each layer of protection to complement the other layers. For instance, most organizations have a strict perimeter firewall that blocks all traffic inbound and outbound except for the specific required ports, such as tcp/80, tcp/443, udp/53, tcp/25, and perhaps a few others. Knowing how their perimeter firewall is configured, an organization should set their HBFW to strictly filter the ports that are allowed by the perimeter firewall. Additionally, there are certain traffic flows that traditional network firewalls can't see based on placement, like local subnet to subnet traffic. The HBFW does not suffer that limitation. For instance tcp/445 is typically used for SMB file sharing. While SMB traffic may be expected between workstations and the file share server, there is usually not a need for a workstation to communicate with another workstation over SMB. Using the HBFW, an organization can block workstation to workstation SMB while allowing SMB traffic to the file server.

HBFW can utilize communication based application whitelisting and/or blacklisting. To maximize security, organizations should use whitelisting.

- Blacklisting: Block specific items.
- Whitelisting: Allow specific items, block everything else.

The best example of this is with tcp/80 (HTTP). TCP/80 will most likely be allowed out of a network firewall as it is required for normal Internet communications. For our DiD model, we would want to complement this network policy with an appropriate host based control. So, what applications really need to communicate out from a host on port 80? The list is probably not more than 20 or so applications: Internet Explorer, Firefox, Chrome, Java, Flash, etc. You may think this list could get long, but for most organizations even without a baseline the number is relatively small. Thus, we would configure the HBFW to only allow the specific applications that are needed to communicate out on tcp/80.

An attacker can still circumvent this control unless it is configured properly. As an example, if an administrator has the HBFW set to only allow outbound tcp/80 when the application is named firefox.exe, the attacker only needs to rename his/her malware to firefox.exe. To counter this, in most HBFWs, an administrator can include more detail in the rule, such as a path name and/or a hash value as well. So now the rule would be: *Only allow outbound tcp/80 when the application is d:\Program Files\Mozilla\Firefox.exe with an MD5 hash of b4c6e3889bb310ca7e974a04ec6e46ac*.

Note that organizations must be careful when utilizing the hash feature, unless Change Control is particularly strong in the organization. This is because every update to an application changes the hash value, thus requiring a corresponding change in the HBFW. For example, if an update for Firefox is pushed out in an automated fashion across the enterprise, but the HBFW is not updated, the browser will not be able to communicate with the Internet until the HBFW rules are modified to allow the new hash. This will be explored more in the application whitelisting section.

At this point it is probably becoming apparent that configuring Endpoint Security products correctly can be very complex. However, the return on investment (ROI) is worth the time utilized in deployment. For example, the single step of configuring application whitelisting for tcp/80 within a HBFW significantly increases the security posture of an organization. The reason this is so valuable is that attackers routinely write malware that communicates with its command and control (C2) server on common ports, such as tcp/80. With the proper HBFW configuration in place, the malware may be able to infect a machine but it would not be able to exfiltrate data or receive new commands, as that traffic would be blocked by the HBFW, rendering the malware useless to the attackers.

14.5.4 Host Based Intrusion Prevention Systems (HIPS)

Intrusion Prevention Systems (IPS) are another familiar network based security technology. Host based IPS, known as HIPS, operate in a similar fashion to their network counterparts, in that they will watch for events that match a specific pattern. The main difference is that with HIPS the focus is shifted to monitoring files, services, and in some cases the registry. With HIPS, organizations can implement rules that alert when a file, process, service or registry object is modified, created, deleted,

or stopped/paused. As with network based IPS, HIPS signatures are usually created to combat a specific attack.

Organizations can utilize vendor-provided signatures and also implement their own custom signatures. One useful and often overlooked feature of HIPS is that custom rules can include rules based on user and service accounts. To understand how this may be useful, consider the following scenarios:

1. System administrators have been caught using a Web browser on a server while logged in with the local administrator account. While browsing the Web from the server, the system administrator accidentally infected the server with malware, which ran with the logged-in user's privileges (local administrator).
2. Skilled hackers were found causing havoc on a network using the Sysinternals pstools that system administrators loaded on the workstations and servers for general troubleshooting tasks.
3. An attacker has been exfiltrating any files with a filename that contains the word password.

Using HIPS, a skilled Endpoint Security Administrator can combat each of these scenarios as follows:

1. Write a HIPS signature that blocks access to iexplorer.exe, firefox.exe, or chrome.exe from the administrator account.
2. Write a signature that only allows certain users to access the pstools.
3. Create a decoy file named passwords.txt and write a signature that will monitor access to this file and report back on the users that attempt to open the file.

With a little creativity, HIPS can be configured to yield extremely valuable results.

14.5.5 Application Whitelisting

We introduced application whitelisting in the HBFW section above, stating that application whitelisting is the technique of allowing specific processes to run, while blocking everything else. In the HBFW section, we discussed how application whitelisting could be utilized to limit communications. In this section, we show how it is used to control whether a process is allowed to run at all.

Application whitelisting can be both the most rewarding technique for security and the most devastating to functionality, depending on how it is implemented. The first item an organization should consider before implementing Application Whitelisting is a baseline. Without a strong baseline and standard build for operating systems, application whitelisting can be a nightmare to configure. To put it in perspective, a base install of Windows XP has a little over 4,000 executables. It is not uncommon for that number to grow to upwards of 20,000 executables on a single XP machine and much higher for Windows 7.

Without a baseline, each host will have its own set of applications, which could quickly bring the total number of unique applications for an enterprise into the hun-

dreds of thousands. The larger the application whitelist becomes, the harder it is to maintain and the more resources it can drain from a host. To assist administrators with building a whitelist and maintaining it, most Endpoint Security products offer multiple features to ease the burden.

The first is a learning mode ability for applications. When learning mode is enabled, the host will report back all the applications that were launched so the Endpoint Security administrators can validate and approve or reject them. There are three main points to consider when running in learning mode—the size of the pool, the duration of monitoring, and whether or not all applications will be used during the learning period. Organizations should focus on a small subset of machines at first to create the baseline and run learning mode for 30 days. This should be long enough to catch most applications that run. Then infrequently used applications that are not run during learning mode can be added to the whitelist later on as needed.

Most application whitelisting products will also allow administrators to choose to automatically approve applications that are signed by a valid certificate from Microsoft and/or security vendors. Flame[7] and Bit9[8] showed how trusting certificates is not always a valid approach though. If a single Certificate Authority (CA) is compromised or decides to support a specific country or interest group, Certificates generated by that entity cannot be trusted. If there were only a few CA's this would not be as concerning, but with hundreds it is not feasible to validate all CAs.

When whitelisting applications, administrators can use the application name, path, and/or hash. Additionally, most solutions allow administrators to choose what applications are allowed for application hooking as well. Application hooking refers to the ability for code to tap into another application or function to view, interact with, or modify that application. The stricter these options are configured, the more secure they make the system, but the harder it is to maintain the operating environment. If baselines are already established, the rewards from a strict configuration will be immense. Malware will not be able to launch on a machine via traditional methods without being on the application whitelist.

14.5.6 Rogue Host Detection

One major limitation with Endpoint Security products is that they need to be installed on each host to be effective. All it takes is a single machine entering the network without the Endpoint Security solution installed to create an incident. To combat this, Endpoint Security products usually include a module for detecting rogue hosts. A rogue host is any endpoint on the network that does not have the Endpoint Security product installed.

[7] http://nakedsecurity.sophos.com/2012/06/07/microsoft-speaks-out-on-flame-malware-certificate-forgery/

[8] https://blog.bit9.com/2013/02/25/bit9-security-incident-update/

Rogue host detection is typically performed by having a couple hosts on each subnet constantly listening and scanning for new hosts on the subnet. As hosts are identified, they are validated to see if they have the appropriate products installed. If not, an alert is raised, or with some products, action is taken to remediate the issue. Mature environments use a solution like this to identify rogue machines, attempt to install security products remotely, and quarantine the rouge machine if the installation is unsuccessful—all handled automatically by the rogue host detection solution. This same process can be used to identify machines that do not have appropriate patches installed, quarantine them until they are patched and then allow them back on the network.

When first identifying rogue devices, administrators will have to make exceptions for devices like printers, VoIP phones, and similar devices. To make this process easier, administrators can exclude MAC addresses that match typical vendor MACs for printers and other peripherals. This will save administrators a substantial amount of time, but could also be leveraged by attackers. For instance if an attacker knows that the general practice is to check the MAC of a rogue device to determine if is a valid peripheral, the attacker can then spoof the MAC address on his/her attacker system to make it look like a printer.

14.5.7 Policy Auditing and File Integrity Monitoring

As mentioned in the application whitelisting section, having a baseline of devices on a network is imperative to securing the devices. A baseline is a snapshot in time of processes, files, registry settings, user accounts, services, and other details on the system. Creating a baseline of hundreds of thousands of machines after they have been deployed is not an easy task. To aid in this task there are Endpoint Security products that will monitor a device for changes to files, services, user accounts, processes, etc. While these baseline monitors will report back to administrators on the changes, they currently expect a human to look at the change that was made and determine if the change was valid. This can quickly become overwhelming if all directories, and files are included in the baseline monitor. To ease administration it may be best for an organization to only monitor specific files and folders that are usually targets, like the system32 directory. This shortcut can lead to an attacker evading detection by making changes to portions of the system that are not monitored. Other important files to monitor are executables, configuration files, and system files.

14.5.8 Data Loss Prevention (DLP)

Organizations are starting to realize that it may be unrealistic to think they can stop 100 % of attacks targeted at their network. With this in mind, some organizations are shifting at least some resources to monitoring for and stopping data exfiltration, thus

taking their security defenses down to the data level. Using DLP tools at the network and host level can hinder attackers from getting the data they want out of the network.

DLP is the process of monitoring and protecting data while in transit and at rest with content aware technologies.[9] Rather than just looking for a file with a specific extension like .doc, DLP can inspect the contents of the file for ASCII strings such as "Confidential", "Classified", "Secret", or even a pattern like three digits followed by a dash, followed by two digits, followed by a dash, followed by four digits (i.e., a social security number).

This is a great method for monitoring and protecting marked documents. Some organizations may benefit from widening parameters of the DLP to monitor all files of a particular type that the organization would like to monitor. This would give the organization an audit trail of all documents in the specified type that were accessed, transferred, or modified. Some DLP solutions can even archive a copy of the file for further analysis.

14.5.9 Device Control

Physical attacks are a large concern in Endpoint Security. While many organizations focus on securing their networks and getting AV and HBFWs tuned, an attacker may be able to walk into an office, plug in a USB device or insert a CD, and steal data or boot to a live Linux distro and carry out an attack. To address this threat, there are Endpoint Security products that fall into the Device Control category. These products monitor and control access to USB ports, CD/DVD drives, and peripherals.

When used in conjunction with DLP products, Device Control solutions can be very powerful. For instance, an organization could implement a policy where only certain users or systems are allowed to write documents with sensitive information to a CD, with all other attempts being blocked. USB control is another great use for this product. Most of these solutions allow for whitelisting or blacklisting of USB devices. Organizations can issue USB thumb drives to specific people and allow only those USB devices to be connected to a system. If additional granularity in the controls is required, the organization can tailor whitelists per endpoint, specifying what peripherals are authorized on that endpoint, which users can access those peripherals, and what actions they can take (read, write, delete, etc.).

14.5.10 Incident Response Agent

Organizations understand that there are going to be intrusions regardless of how well protected they are. Responding to these incidents effectively can be the difference between an attacker being eradicated from the network with little to no damage

[9] https://securosis.com/research/research-data-loss-prevention

and a major incident involving a large data breach and negative publicity. An incident response product can quickly gather data from a compromised host to use within an investigation. These tools pull information such as the list of running processes, a list of established network connections, DNS cache information, memory dumps, event logs, and even full images of the machine. Some of the tools in this category allow incident responders to run commands and tools remotely to gather data that is not already available natively through the product.

14.6 Am I Safe Now?

With the strictest policies and practices implemented within all of these tools, organizations will still be attacked and potentially compromised. There is no 100 % solution for network or Endpoint Security. That is the unfortunate reality of the current ever-evolving threat landscape. This is why DiD solutions must complement each other to provide a more holistic approach to an organization's security. There are many evasion tactics, some of which are outlined in the sections above. Additionally, as stated above, effective Endpoint Security relies on each host having the full solution installed, configured, and running properly. If the firewall service crashes, or a host is not configured properly, the affected machine may be compromised if another piece of the solution does not catch and mitigate or remediate the issue. That is why it is important to have all of the pieces working in concert. Following the guidance in this chapter, organizations can stop a vast majority of attacks. Additionally, organizations will be in a better position to detect and respond to attacks that do occur, while reducing the risk of adverse effects and future compromises.

Bibliography

Ducklin, P (2012) Microsoft speaks out on Flame malware certificate forgery. Retrieved 29 Nov 2103, from Naked Security: http://nakedsecurity.sophos.com/2012/06/07/microsoft-speaks-out-on-flame-malware-certificate-forgery/

Lambert, P (2013) New controversy on the effectiveness of antivirus software. Retrieved 29 Nov 2013, from TechRepublic: http://www.techrepublic.com/blog/it-security/new-controversy-on-the-effectiveness-of-antivirus-software/8919/

McAfee (2013) Supported environments for Common Management Agent and McAfee Agent 4.x. Retrieved 29 Nov 2013, from McAfee Knowledgebase: https://kc.mcafee.com/corporate/index?page=content&id=KB51573

Microsoft (2013) Virus scanning recommendations for Enterprise computers that are running currently supported versions of Windows. Retrieved 29 Nov 2103, from Microsoft Support: http://support.microsoft.com/kb/822158

Muncaster, P (2013) Symantec: Don't blame us for New York Times hack. Retrieved 29 Nov 2013, from The Register: http://www.theregister.co.uk/2013/02/01/symantec_responds_nyt_apt/

Securosis (2009) Research: Data Loss Prevention. Retrieved 29 Nov 2103, from Securosis: https://securosis.com/research/research-data-loss-prevention

SVERDLOVE, H (2013) Retrieved 29 Nov 2013, from Bit9 Blog: https://blog.bit9.com/2013/02/25/bit9-security-incident-update/

Symantec (2013). Annual Symantec Internet Security Threat Report Reveals 81 Percent Increase in Malicious Attacks. Retrieved 29 Nov 2013, from symantec.com: http://www.symantec.com/about/news/release/article.jsp?prid=20120429_01

Tung, L (2012) How much malware has arrived since 1984? Retrieved 29 Nov 2013, from CSO: http://www.cso.com.au/article/419622/how_much_malware_has_arrived_since_1984_/