VOLUME 1 (2015) ▪ ISSUE 1

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

ANALYSES ▪ POLICY REVIEWS ▪ OPINIONS

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

The European Cybersecurity Journal is a new specialized quarterly publication devoted to cybersecurity. It will be a platform of regular dialogue on the most strategic aspects of cybersecurity. The main goal of the Journal is to provide concrete policy recommendations for European decision-makers and raise awareness on both issues and problem-solving instruments.

EDITORIAL BOARD

ISSN: 2450-2111

Published by:
The Kosciuszko Institute
ul. Lenartowicza 7/4
31-138 Kraków, Poland

Phone: 00 48 12 632 97 24
E-mail: editor@cybersecforum.eu

www.ik.org.pl
www.cybersecforum.eu

The ECJ is a quarterly journal, published in March, June, September, and December.
The first issue of the ECJ is free of charge.

THE KOSCIUSZKO INSTITUTE

Citations: This journal should be cited as follows: "European Cybersecurity Journal", Volume 1 (2015), Issue 1, page reference

PUBLICATION PARTNERS

NATO OTAN

The first issue of the ECJ is co-sponsored by the North Atlantic Treaty Organization.

Ministry of Foreign Affairs Republic of Poland

The first issue of the ECJ is co-financed by the Ministry of Foreign Affairs of the Republic of Poland within competition: „Support for local government and citizen dimension of the Polish foreign policy 2015".

Consulate of the United States of America

The first issue of the ECJ is co-sponsored by the Consulate of the United States of America

Printed in Poland
by Drukarnia Diament | diamentdruk.pl

DTP: Bartosz Borczuch

Disclaimer: The views expressed in articles are the authors' and not necessarily those of the Kosciuszko Institute or any of the publication partners. Authors may have consulting or other business relationships with the companies they discuss.

EDITORIAL

JOANNA ŚWIĄTKOWSKA
Chief Editor of the European Cybersecurity Journal
CYBERSEC Programme Director
Senior Research Fellow of the Kosciuszko Institute, Poland

Cybersecurity and, more broadly, issues connected with cyberspace, have risen to the rank of strategic, global challenges. On the one hand, over the last few decades we have witnessed unprecedented opportunities for general development: economic, political, social, and individual. On the other, we are now facing completely new categories of threats, with potentially catastrophic consequences. All stakeholders, even the non-governmental ones, who, in the past, had limited or no tools enabling them to effectively influence the world around, now have comparatively easy access to technologies that may potentially impact entire international security systems. The Web has become a tremendous source of influence.

In order to safely use and develop the potential of cyberspace, global collaboration and engagement of all stakeholders are absolutely necessary. Europe is an extremely important element of this ecosystem and should be actively engaged in all processes affecting global cybersecurity. One of the key steps necessary for developing the best ideas and the most practical solutions is to create a platform where different points of view can be presented, confronted, and debated.

The European Cybersecurity Journal offers different perspectives on cybersecurity management and related public policies. The main goal of the ECJ is to provide concrete policy recommendations for European decision-makers and raise awareness on key issues and problem-solving instruments. The first edition of the quarterly will be officially inaugurated during the European Cybersecurity Forum (CYBERSEC) – the project which aspires to become the most important European discussion platform for cybersecurity and related strategy challenges.

Both the ECJ and CYBERSEC have been designed to support the general effort of increasing security and promoting stable growth opportunities across cyberspace.

In the process, we have decided to include all key stakeholders: representatives of public entities, business leaders, experts, scientists, and representatives of the civil society. Bringing together so many diverse points of view is our core value. It also makes us stand out when compared to other projects addressing this subject matter from, for example, exclusively technological perspective.

The first issue of our quarterly provides a clear illustration of this approach. It covers some of the boldest and most innovative solutions, presented from a variety of perspectives. This unique approach ensures new levels of insight into some of the most crucial cybersecurity issues, presented in the form of analyses, interviews, opinions and policy reviews.

It gives me great pleasure to share with you this very first edition of the ECJ. In it, I hope you will find valuable reading material, useful practical information but also many sources of inspiration. At the same time I would like to invite you to contribute to the development of our journal. In line with the fundamental nature of the Internet itself, the value that a multi-stakeholder approach creates, can only materialize if it is driven by a collective effort. This particular effort offers a promise of a better, safer future, in which cyberspace continues to provide unprecedented development opportunities, at personal as well as international level.

Joanna Świątkowska

CONTENTS

CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

EUROPEAN CYBERSECURITY FORUM - CYBERSEC

JOANNA ŚWIĄTKOWSKA
Joanna Świątkowska is the Senior Research Fellow for Cybersecurity of the Kosciuszko Institute and the Programme Director of CYBERSEC. She is the Chief Editor of the European Cybersecurity Journal. She has been involved in numerous high profiled national and international cybersecurity initiatives. She often cooperates with Polish public institutions, including, among others, the Polish Presidential National Bureau of Security (NBS). In the framework of the National Forum of Security organized by NBS, she contributed to the cyber doctrine of Poland. She also advised the Supreme Audit Office in terms of cybersecurity control in Poland. She took part as an expert in the Sino- European Cyber Dialogue held in Geneva and Beijing in 2014. She is the author of numerous articles, reports and analyses concerning cybersecurity, such as a recently published report on critical infrastructure cybersecurity in Poland. She defended her doctoral dissertation in the field of political science. She has been selected for the U.S. Department of State's International Visitor Leadership Program (IVLP) on "Cyber Security and Government Interoperability" taking place in 2016.

CYBERSEC – a new platform for strategic talks on cybersecurity

Cyberspace and especially problems related to its security are becoming a subject of discussions on the highest national or international level. Such discussions should involve all the stakeholders: top-level managers, governmental and military officials, European-level representatives, academics, and civil society. Ensuring cybersecurity does not only entail skill and technical know-how, but currently an equally significant and necessary role plays appropriate strategic political action.

In a world where the most important players are already creating the processes which will decide the future of cyberspace, the voice of Europe must be heard. The "cyber element" of the conflict in Ukraine, the NATO Summit in Warsaw during which one of the priorities will be the issue of cybersecurity, the undergoing work on some of the most important EU legislative solutions, and the transatlantic trust crisis caused by the Snowden revelations are all topics which show that security in cyberspace is becoming a key issue. Security, however, is something that is built collectively, therefore it is essential to provide a forum for all the cyberspace stakeholders to meet and debate. Kraków is an ideal place for such meetings and Poland, due to its geopolitical location, understands the challenges of the future. In turn, Central Europe has until now been insufficiently involved in matters related to cyberspace.

CYBERSEC will involve our region in the global debate, as the European Cybersecurity Forum aspires to create new concepts, ideas, and solutions. CYBERSEC will also continuously support the development of competences and capabilities in the field of cybersecurity, engaging academia, experts, and business environments of large and medium companies, as well as start-ups in the process. It is essential to create cooperation between science and business in the areas of education, higher learning, and transfer of knowledge and technology.

CYBERSEC is divided into four streams focusing on key issues pertaining to cyberspace: state, military, future, and business stream.

Illustration 1. Four topical streams of the European Cybersecurity Forum.

CYBERSEC is a year round project. Before the Forum the participants join in preparatory webinars, and after the conference, a set of recommendations will be prepared for each topical stream, which will then be promoted among the specially selected, key target groups. We will repeat this process every year with the intention of inspiring politicians to implement the best solutions that raise the security of the entire Europe, and also to build lasting trust and understanding among the partners.

Each edition of CYBERSEC will touch on the most current cybersecurity topics on the international agenda. The selection of the participants, on the other hand, will guarantee a broad spectrum of opinions and positions of key stakeholders. At the same time, we will maintain the balance between the need to strengthen security and ensuring conditions favourable to innovation, as well as respecting individual rights of citizens.

Cybersecurity of both Poland and Europe demands continuous development of stable relations and long term partnerships, for which CYBERSEC provides a perfect venue. We are convinced that thanks to its merits, our conference will become a permanent fixture on the calendar of key security events.

This project is not only hard work, but also a great adventure. Many key public and academic institutions, as well as representatives of business have already joined us. We invite anyone willing to cooperate to get involved as well. ■

CYBERSEC FORMULA

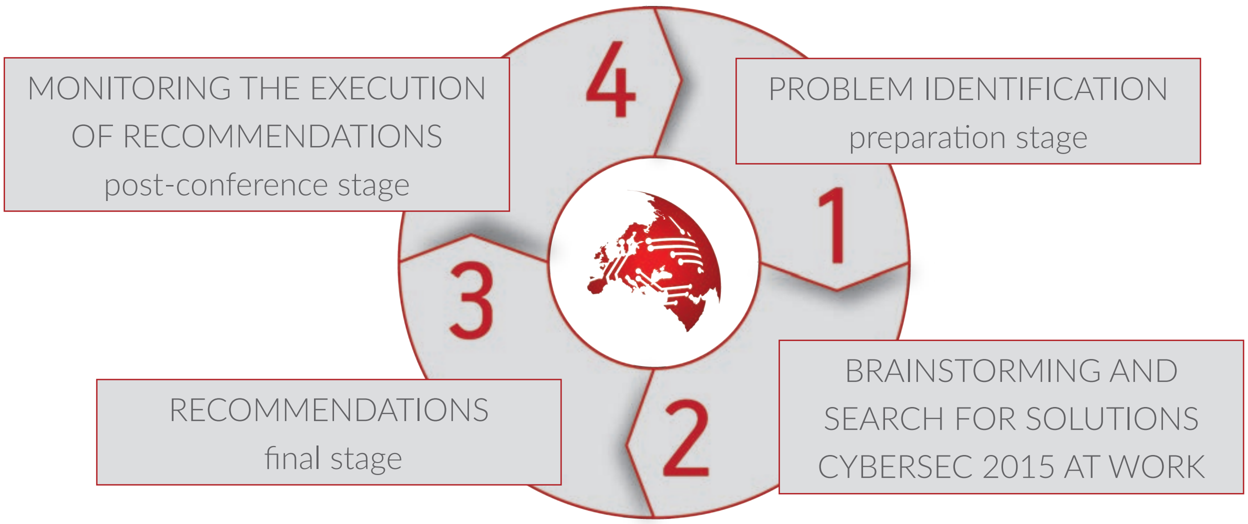


Illustration 2. Stages of work.

INTERVIEW WITH DR JAMES ANDREW LEWIS, HONORARY MEMBER OF THE EDITORIAL BOARD OF THE ECJ

DR JAMES ANDREW LEWIS

James Andrew Lewis is a Senior Fellow and Program Director at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked at the Departments of State and Commerce. He was the advisor for the 2010, 2013 and 2015 United Nations Group of Governmental Experts on Information Security and led a long-running Track II dialogue on cybersecurity with the China Institute of Contemporary International Relations. Lewis has authored many publications and is an internationally recognized expert on cybersecurity. He has testified numerous times before Congress and is frequently quoted in the media. Lewis received his Ph.D. from the University of Chicago.

Dear Dr Lewis, this is an honour for the European Cybersecurity Journal to count you as the Honorary Member of its Editorial Board.

Currently many processes influence the strategic developments related to cybersecurity in Europe. Considering your experience in similar processes which have taken and are still taking place in the United States, I would like to ask for your opinion on some key-issues on this subject.

The Network and Information Security (NIS) Directive, currently negotiated, will most probably introduce some obligatory responsibilities for various stakeholders, including in the area of public-private cooperation. This is one of the most questionable aspects of the Directive, as well as a novel approach for many Member States (e.g. Poland). At the same time in the USA, the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) and consulted with the private sector is functioning for one and a half year and is being called a voluntary tool. Do you think of the Framework as useful? Is it possible to assess its effectiveness in enhancing security?

It is too early to tell how successful the NIST Framework has been, but it does give companies a benchmark and guidance for their cybersecurity efforts. It is important to note that the Framework is not entirely voluntary. The Executive Order tasks regulatory agencies in areas like finance, telecom, and electrical power, to ensure that their existing regulations are adequate for cybersecurity and implement the Framework. The degree of voluntary action varies from sector to sector. The threat or regulation has also been effective as an incentive. What companies worry about is being locked into a static regulatory framework when the threat they face is dynamic.
There is another aspect that should be underlined: Even if companies fully implement the NIST Framework (whatever that might entail), it does not necessarily mean that there will be an improvement in cybersecurity. The measures listed by NIST are likely to improve security, if implemented correctly, but to what degree is unknown. The only way to accurately measure effectiveness is to ask if the number of successful penetrations and the outflow of data decreased. If hackers still get in and data still flows out, the Framework is not working.

Finally it is worth to mention that NIS does not provide guidance on implementation – and the implementation phase is a crucial part of the process.

How does inter-sector cooperation work in the US, especially between major industries in critical infrastructure sectors like energy or transport? Do owners and operators work together? What would be the best recommendations in this field? May the state effectively support the information exchange mechanisms?

There is not as much cross-sectoral work as you might think. The Department of Homeland Security has done some work to bring sectors together, but the most success seems to be at the local/state level, where critical infrastructure companies recognize their interdependence – no water means no electricity, no electricity means no phones, and so on.

In your opinion (basing on the US experience), which deterrence strategies or tools would be most effective as possible reactions to the cyber conflicts which are below cyberwar's threshold (i.e. do not cause disturbances in the constitutional order or life and massive material losses)?

Deterrence does not work for actions below the threshold of armed conflict, and nations have adopted tactics – including cyberattack – to circumvent deterrence. We face new kinds of opponents and a new strategic environment, and need alternate solutions to set limits and create credible threats. Whether this is active defense or something else remains to be determined, and the US is currently trying to define "proportional response" so that it can make credible threats in cyberspace, but deterrence has not worked as it is currently structured. This is something I am working on now.

In your opinion, how can we rebuild trust in the transatlantic relationship, recently eroded by the information disclosed by Edward Snowden?

Snowden's leaks revitalized the European left, which had been despondent since the collapse of communism, and accelerated the discontent created by the intervention in Iraq. That said, I do not think the transatlantic community has a choice. The US needs to cut back on spying on European partners (it is largely a waste of time), but the EU needs to recognize that a world shaped by Russia and China may be much less pleasant for them. There is an old American saying that we can either hang together or we will hang separately, and it applies in this case.

The cyber-insurance market is much more developed in the United States than in Europe. How would you assess the usefulness of such tools in order to increase the level of cybersecurity?

Insurance is pretty useless as people don't have good actuarial data on risk and how to reduce it. Once there is enough data on how to manage risk, insurance can become more valuable. As the market matures, insurance can play a greater role in shaping company decisions.

Thank you for this inspiring interview which opens a series of articles on cybersecurity management and public policies in the first issue of the ECJ. ■

Questions by Joanna Świątkowska,
The Kosciuszko Institute

ANALYSIS

CYBERSECURITY GOVERNANCE - THE NEW GOVERNANCE PARADIGM

HELENA RAUD

Helena Raud has 10 years of experience in defence planning and consultancy. She re-profiled to cybersecurity following the 2007 attacks against Estonian private and government sites. She is a co-founder and Board Member of the European Cyber Security Initiative, a NGO that has taken to heart developing a virtual environment for conducting strategic level cyber exercises. As an academic, Helena Raud is interested in technology dependence, connections between innovation and economic development and the role of governance. Former Cyber Security Co-Ordinator for Estonia, leading the work on the Estonian Cyber Security Strategy for the period 2014-2017.

The rise in the use of different technologies over the 20th and the start of the 21st century has been vast. From the use and development of personal computers and mobile phones, to internet-based services provided by states and private companies, to management of industrial control systems, technology has changed the way we live. Today's world is a world of high-tech, of the ICT revolution[1] and e-society where the Internet is the primary and usually the most cost-effective source for information[2]. While being an almost global trend, this is mostly true in developed societies which embraced the new "techno-economic paradigm"[3], which started with the evolution and the widespread use of the microchip, that evolved into the ICT revolution[4] and societies' and states' ability to enjoy overall high levels of technological skills and knowledge in the West.

However, there is a downside to this almost incomprehensible amount of freedom and access to information and decision-making tools that the society has never before experienced. Cyber incidents either stemming from criminal action of individuals, state-sponsored organisations, or human and technical error have risen from being just an issue for large corporations providing services closely tied to ICT means[5], to a topic

[1] | Perez C., Technological Revolutions and Financial Capital – The Dynamics of Bubbles and Golden Ages, Edward Elgar 2002, p.18.

[2] | Magretts, H., The Internet and Public Policy, "Policy & Internet", Vol. 1: Iss. 1, Article 1, Berkeley 2009, p. 5 ;
Castells M., Communication Power, Oxford University Press, Oxford 2009, p. 418.

[3] | Op. cited Perez pp. 49-59.

[4] | Ibid

[5] | Loader B. (ed.), The Governance of Cyberspace: Politics, Technology and Global Restructuring, London: Routledge 1997
Cebula J.J., Young L.R., A Taxonomy of Operational Cyber Security Risk, Software Engineering Institute, Carnegie Mellon, 2010 ;
Strategic Foresight Initiative, Technological Development and Dependency-Long-term Trends and Drivers and Their Implication for Emergency Management, FEMA May 2011, p. 4.

on top of the list of most governments in the Western World. Risks involved in disregarding possibilities of further and more developed cyber incidents, and inaction of states to increase readiness to deal with such risks, could result in not just an inconvenience for the people, but major economic losses and even loss of life[6].

The impact of breaches of information systems and cyberthreats resulted in policy action after the large scale cyberattacks on Estonia's government and private sector websites in April 2007[7]. The essence of the attacks was rooted in the hostility of a small interest group, but showed the ease of which both the legitimacy of a state can be affected by the use of ICT and the magnitude of societal dependence on information systems beyond that of media or communication[8].

The ever-increasing societal dependence on technologies further increases the likelihood of cyber incidents with significant socio-economic impact, as individuals, businesses, and the government continue to move more services on-line.

While the implications of inaction by governments to tackle cyber risks have become clear through the incidents in 2007 in Estonia, or subsequently in Georgia, Germany, or the US[9], and many countries since, governments face challenges with applying new policy-making and governance principles into practice[10]. It is important to consider that cybersecurity did not arise solely as a response to a single event (or series of events), but due to persistent cyberthreats and thus cybersecurity governance must remain an on-going government process.

The problems in cybersecurity governance manifest themselves on several levels: the inability to define the scope of cybersecurity, of creating holistic policies that would take into account all the consumers of cybersecurity, considering all types of cyberthreats, providing clear roles for government agencies, establishing effective private-public cooperation and specifying the budgetary means necessary for implementation of cybersecurity policies.

In Estonia, the emergence of the cybersecurity governance paradigm arose after the 2007 cyberattacks that are internationally considered as the first cyberwar[11]. Due to the successful mitigation of the attacks in 2007 and the creation of a seemingly holistic cybersecurity strategy, Estonia became one of the world's leading experts in government level cybersecurity. However, Estonia has also been criticised for an overly New Public Management-driven approach to public management that has led to dependence on out-sourcing government tasks and a thin public sector unable to implement policies[12].

Another cause for concern is the misinterpretation of security in cybersecurity. If cybersecurity is viewed from a narrow national defence perspective, a negative impact will be created through unwillingness of government agencies, outside of ministries of defence, to take action in cybersecurity policy creation, implementation, and financing. The effects of government inaction in cybersecurity policy implementation can have serious socio-economic implications. Sectors such as energy, telecommunication, and finance are all interlinked and rely on the functioning of "interdependent networks of information systems"[13]. The spill-over effect caused by a disruption of one of the service sectors has direct impact on other vital services and on operations of businesses and individuals in general.

Similarly, government provided e-services rely on the functioning of the same critical services, with direct negative impact of information systems disruptions on citizens' welfare. For private individuals, the effects

[6] | Kelly J. J., Almann L., eWMDs, "Policy Review", Hoover Institution, Stanford University 2008/2009
Herzog S., Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, "Journal of Strategic Security", Vol. 4, Issue 2, Henley-Putnam University Press 2011

[7] | Ibid

[8] | Ibid ; Op. cited Castells, p. 418.

[9] | Op. cited Kelly, Almann and Herzog

[10] | Kitsing M., An Evaluation of E-Government in Estonia, "Internet, Politics and Policy 2010: An Impact Assessment" conference, University of Oxford, 2010 ;
Mistra D. C., Ten Guiding Principles for E-Government, UNPAN 2009, p. 3 [online] www.unpan1.un.org (access: 10.05.2012)

[11] | Lander M., Markoff J., In Estonia, What May be the First War in Cyberspace, "The New York Times", 2007, [online] www.nytimes.com, (access: 10.05.2012)

[12] | Randma T., A Small Civil Service in Transition: The Case of Estonia, "Public Administration and Development", Volume 21, Issue 1, pp. 41–51, February 2001 ;
Drechsler W. (2004), Governance, good governance, and government: The case for Estonian administrative capacity, TRAMES, 2004, 8 (58/53), 4, pp. 388-396.

[13] | Buckland B. S., Schreier F., Winkler T.H., Democratic Governance Challenges of Cyber Security, DCAF Horizon 2015 Working Paper no 1, 2011, p.9 [online] http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security, (access: 10.05.2012)

of criminal or negligent abuse of information systems may cause the most significant effect, starting from damage or misuse of their personal information, to the inability to use communication means to access emergency services, or loss of access to their funds.

1. The Definition

The discourse on cybersecurity is made complex as there is no universal definition of cybersecurity. The DCAF Horizon 2015 Working Paper defines cyberspace as the "interdependent network of information technology infrastructures"[14]. Thus, for the purposes of this article cybersecurity will be defined as security of "interdependent network of information technology infrastructures" that can be further divided into sub-categories of: cyberdefence, combatting cybercrime and critical information infrastructure protection (CIIP). The definition of cybersecurity can be widened by specifying three distinct areas that cybersecurity should address: protection measures in IT, the level of actual protection achieved, and the professional efforts invested into protection of cyberspace[15].

> “ The challenges and significance of cybersecurity governance and defining cybersecurity itself arise from the multitude of users of different technologies.

The challenges and significance of cybersecurity governance and defining cybersecurity itself, arise from the multitude of users of different technologies. As it was mentioned, the user groups span from private individuals to businesses to governments, and the interaction is almost never one-way. It is this interaction, which can be harmed through cyber means on services, such as telecommunications, energy provision, and provision of other critical services and common utilities. With an agenda as varied as it is described in the definition of cybersecurity, the security element in the definition bears much more significance than it does in the common approach to national defence/ security by governments.

The fact that national defence has historically dealt with the physical threats to the integrity of the state and the lives of the citizens is not irrelevant to cybersecurity, but emphasising the defence agenda of cybersecurity does not create opportunities for the development of national institutions, tasked to handle cyberthreats, outside of defence organizations. A direct effect of viewing cybersecurity from a military defence stand-point, could be the neglect of the obligation that states must provide resilience of information systems at peace-time or create measures that would prevent social unrest and anti-government action in instances where the threat comes from disruptions in provision of critical services or even convenience utilities such as access to mobile Internet or digital television.

1.1 The Concept Of Securitization

Considering the complexity of the cybersecurity agenda, the significance of the securitization process needs further explanation. In fact, it is not a mere choice of words in terminology, but similarly to social security or energy security, it sets greater requirements for public management organizations and performing of state duties for its citizens and businesses.

Securitization means that any phenomenon with significant impacts on societal welfare, which can be impacted through internal or external threats, can be and ought to be made a priority[16]. Government action through securitization of an agenda requires creation of specific policies and assigning institutional responsibilities to government agencies[17], on the one hand, with the task to protect the constitutional rights of the citizens, and on the other hand, to create legal and regulatory measures to ensure adequate responses to the threats[18].

[14] | Ibid

[15] | Fisher E. A., Creating a National Framework for Cybersecurity: An Analysis of Issues and Options, CRS Report for Congress, The Library of Congress, USA 2005, p. 19.

[16] | erez C., Technological Revolutions and Financial Capital – The Dynamics of Bubbles and Golden Ages, Edward Elgar 2002, p.18.

[17] | Ibid

[18] | Ibid

Securitization in the broad sense was described by Buzan, who admits that military threats are seen as a primary disruptor to national security[19]. However, he also introduces an approach encompassing political, societal, economic, and environmental threats as aspects of national security[20].

The concept of securitization itself was reaffirmed by Ole Weaver, simplifying the emergence of topics from everyday life into political discourse, and assuming them as threats, by stating that "something is a security problem when the elites declare it to be so"[21]. Thus, not all securitized agendas can be directly classified as matters of military or national defence, but for threats to be securitized, governments must accept them as significant.

1.2 Securitizing Independent Networks Of Information Technology Infrastructures Or Cyberspace

Securitizing "interdependent networks of information technology infrastructure" is the first and most valuable element to understanding the emergence of cybersecurity into the policy realm in states[22]. To this end, the combining term for "independent networks of information technology infrastructures" – cybersecurity, was introduced[23]. Securitization, as it is argued here, is not so much an event, but a process, where the severity and complexity of impact of threats undergoing securitization, necessitate the creation of holistic multi-layer policies and strong organizational governance structures by states.

The nature of cybersecurity, a field so interdisciplinary, naturally touches heavily upon national defence and cannot thus be undermined, but securitization, misinterpreting, and disregarding the holistic non-military securitization approach of Weaver and Buzan seems prevalent and counterproductive[24]. It is a way of looking at the events in the cyber realm from a narrow perspective that can be often observed in political science, where complex societal issues are narrowed down to fit certain criteria, certain theories, or methods of scholarly inquiry, while disregarding the complexity of the subject matter and the unpredictability of the actions of associated variables[25].

As stated, the materialization of large-scale cyberthreats does create a legitimate reason, following the principles of Buzan, for the current securitization of cyber[26]. In most instances, like in the case of Estonia that will be elaborated on later, this stance was not incorrect as cyberattacks had occurred following events filling both Weaver's and Buzan's criteria for securitization[27].

In cybersecurity this means that all threats: technical, human action related, and external threats must be evaluated[28]. Furthermore, all cybersecurity threats must be assessed through the impact of spill-overs of cyberthreats against one industry or one service into the next. If the threat dynamics presented by the materialised cyber risks create such impact that all participants in the "physical base of the state" [29] are affected, political level securitization of cyberthreats must be considered and policy action taken.

The understanding of the emergence of cybersecurity, following the securitization theory, is the basis for government's cybersecurity policy action and creates a framework for evaluating the adequacy of public management organizations in relation to the needs of cybersecurity clients. Specifically, the understanding of the scope of securitized cyber, allows for a critical view of New Public Management and Digital Era Governance, and ideology-derived capacity of states to handle the full spectrum of cyber risks and target all necessary interest groups – the general public, businesses, the state, and technology itself.

[19] | Op. cited Buzan, p. 117.
[20] | Ibid ; Op. cited Buzan, pp. 118-134.
[21] | Weaver O., Securitization and Desecuritization, [in:] On Security, ed. Lipschutz R., Columbia University Press 1998, p. 6.
[22] | Op. cited Buckland et al, p. 9.
[23] | Ibid
[24] | Greers K., Strategic Cyber Security, CCD COE Publications, Tallinn 2011
Tenusar E., Responses to Changing Nature of Threats and Security: Analysis of Cybersecurity Initiatives in Estonia and the United Kingdom, University College London 2011; Op. cited Lander, Markoff
[25] | Drechsler W., Understanding the problems of mathematical economics – A "continental" perspective, Real-World Economic Review, Issue no 56, 2001, pp. 47-48.
[26] | Op. cited Buzan, pp. 118-134.
[27] | Op. cited Weaver, p 6 ; Op. cited Buzan, pp. 118-134.
[28] | Op. cited Cebula, Young ; Op. cited SFI, p. 4.
[29] | Op. cited Buzan, pp. 118-134.

2. Policy Responses And Measures

With securitization of a certain phenomenon, the governments have made it a priority to minimise specific threats. As it is evident that there is a basis for securitizing cyber, from the broadest sense of securitization, proportional policy and regulatory measures should be created. The challenge for governments in addressing policy creation in cybersecurity lies in several factors: first of all, the subject matter of the policy, and whether it should be addressing technological or human aspects of threats, and secondly, whether existing public administration organisations are equipped with the required expertise for successful implementation of cybersecurity policies in order to minimise the effects of cyberthreats.

> “ The understanding of the scope of securitized cyber allows for a critical view of New Public Management and Digital Era Governance.

Broadening the scope of measures, a completely “new regulatory paradigm” should be devised[30] that ought to find a balance between availability of services and freedom of speech with security measures for information systems to be integrated into “any system of regulation”[31]. We have to keep in mind that any proposed regulation is not a solution in itself but must possess a required level of scope, in order to be effectively enforceable[32].

To clarify national policy and contingency planning to tackle cybersecurity risk, ENISA (European Network Security Agency) proposes a set of steps that begin with building an understanding of threat scenarios, of designing specific objectives, structures, and roles (ENISA 2012, III). The framework assumes that the above steps should be used in governance and contingency planning that covers also resource and process planning[33]. Specific focus is targeted at training, testing, and exercising to increase both systems resilience and personnel competence[34]. Furthermore, this type of contingency planning should not be considered a one-time measure but should undergo constant review and modification to ensure “continuous improvement” in cybersecurity (ibid)[35].

After strategic cybersecurity goal-setting by governments, the use of the Doyle and Morris model for suggesting methods for successful internet regulation is necessary. This is based on national, international, and global codes and regulations[36] and the urgent need for new types of regulation since “the internet and other networks do not abide by old regulatory models of nations states, based on national boundaries”[37]. Next to adaption of, for example, criminal law, soft approaches to regulation are also supported in the form of awareness raising activities, sharing information of potential risk, and proposing safety measures, conducted by states[38].

In practice, devising holistic new policies for an agenda that has been securitized through actual events, also means that simply stating the necessity for a new approach to policy and policy enforcement is insufficient. Next to politicians emphasising the importance of the newly securitized agenda, expert policy writers and scholars must revisit the basic criteria that successful new policies would have to meet.

One of the excellent examples to this approach is presented by Fisher, addressing specific challenges and key aspects regarding cybersecurity governance, in a report directed to the US Congress[39]. He stresses that the underlying key to success should “involve establishing clear and measurable goals, strategies for achieving those goals, and policies and procedures to implement those strategies”[40]. When establishing goals, either a path of ultimate decrease in incidents or incentive setting should be used[41].

[30] Groebel J., Metze-Mangold V., van der Peet J., Ward D., Twilight Zones in Cyberspace: Crimes, Risk, Surveillance and User-Driven Dynamics, Friedrich-Ebert-Stiftung and European Institute for the Media, 2001, p. 83.
[31] Ibid
[32] Op. Cited Groebel et al, p. 84.
[33] Ibid ; Op. cited Fisher, p. 21.
[34] Ibid
[35] Ibid
[36] Op. cited Groebel et al, pp. 83-84.
[37] Op. cited Groebel et al, p.85.
[38] Ibid
[39] Op. cited Fisher, p. 17.
[40] Ibid
[41] Ibid

In terms of governance, however, it also needs to be pointed out that next to strategic goal setting, setting and implementing specific policies, related procedures and, most importantly, people management must be incorporated[42]. Moreover, the necessity of clear structures, as opposed to decentralization, must be realised, whereby avoiding distributed responsibilities that could result in "that the issue is not properly addressed by anyone"[43].

However, successful securitization, does not simply rely on acceptance or acknowledgement of certain types of threats, nor can risks be minimized or eliminated through creation of seemingly holistic strategies, policies, and regulations. The key to success lies in the ability of the states to apply policy and continuously meet newly emerging needs of societies in an ever--changing environment of threats. To this end, the choice of governance instruments or paradigm can create either opportunities or challenges for cybersecurity policy implementation, and insurance of cybersecurity by states, as seen in the following comparison of New Public Management and contesting Digital Era Governance.

3. Cybersecurity In Estonia

E-government, e-parking, e-health, e-school, e-taxes, e-banking, e-voting are but a few e-services that Estonian's have the ability to use. In fact, some 98% of Estonians under 35 use the Internet on a regular basis. The users have a very high expectation of e-services and often do not even realize the amount of e-solutions they uses on a daily basis. This can be seen through the statistics published by the OECD where Estonia seems to have a surprisingly low use of e-commerce.

Even without introducing the further cybersecurity threat vector that includes the provision of critical services, such as energy, healthcare, communications, or transportation, it is evident that technology dependence in Estonia can be considered as substantial. However, in order for governments to take consideration of the negative impacts of technology dependence regarding the information society, scholarly or technical advice alone could be insufficient[44]. Following the Buzan-Weaver concept of securitisation, long-term political and administrative considerations concerning a newly emerged threat would only be embedded in the policy realm after the materialisation of a related threat[45].

While measuring successful implementation of cybersecurity strategic objectives is a subjective matter, due to Estonia's increasing technology and e-service dependence, setting up the Cyber Security Council is an effective evaluation tool. According to the strategy, "the Council will monitor the success of the strategy by submitting annual report to the government which will detail the progress of implementation and the realisation of the objectives set out in the implementation plans"[46]. Another positive aspect of the Estonian Cybersecurity Strategy (ECSS) is the ability to ensure flexibility and adaptability based on cybersecurity risk by splitting strategic implementation into two planning periods[47].

Despite policy level prioritization of development of e-services and e-society, Estonia's e-governance has been critiqued for not being applied evenly across the government sector[48]. Moreover, Kitsing argues that the Estonian government lacks a coherent and holistic plan of action or an understanding of the co-operation partners within the state and the private sector[49].

According to this view, action is taken on a more personal or visionary basis and is characteristic of some government agencies but not of a "centralized effort"[50]. Previous studies show that policies created, have not always been backed by institutional change or development[51] and, more importantly, there is a scarcity of subject matter experts in all researched fields[52].

[44] | Heldman R. K., The Telecommunications Information Millenium – A Vision and Plan for the Global Information Society, Computing McGraw-Hill 1995
[45] | Op. cited Buzan, pp. 118-134. ; Op. cited Weaver, p. 6.
[46] | Ibid
[47] | Ibid
[48] | Op. cited Kitsing
[49] | Ibid
[50] | Ibid
[51] | Op. cited Randma, p. 42.
[52] | Op. cited Randma, p. 42.

By this assumption, cyber risk management creates the necessity to either significantly increase the subject matter expertise on all government levels or outsourcing. Furthermore, in order to ensure cybersecurity expertise building in public administration, regulatory change must be developed and implemented because no responsibilities or resources would otherwise be allocated. However, outsourcing tasks that require expertise in cybersecurity would create an even higher risk, as governments would lose further understanding of the technical implications of technology dependence and cybersecurity risk to e-services or even critical service industries.

Cybersecurity governance in Estonia is ensured through co-ordination by the agencies mentioned in the ECSS. The co-ordinating body for co-operation is the Cyber Security Council, a sub-council of the National Security Committee of the Government. Agencies under the specific ministries perform tasks specified by the ministries through their statutory obligations and/or tasks specified in strategic action plans.

In principle, this division of capacities should ensure setting, adopting, and review, as well as, supervisory capabilities. Institutional change and statutory revision was presented as a key to settling policy gaps by the ECSS in order for Estonia's cybersecurity policy to be considered comprehensive, in regard to the Fisher criteria[53]. Furthermore, institutional change was seen as a pre-requisite for governments' ability to use the tools specified by Magretts[54].

> “ In principle, this division of capacities should ensure setting, adopting, and review, as well as supervisory capabilities.

As outlined in the previous section, Kaska points out the need for regulatory change governing the "organization of the state", that would mean the revision of statutes of ministries and other government agencies and inclusion of cybersecurity tasks. However, there is little evidence of such change since 2007[55]. According to the Government Action Plan 2015, the co-ordination of cybersecurity and the lead co-ordinating role in the ECSS 2014 was handed to the Ministry of Economic Affairs and Communications (now Economic Affairs and Infrastructure) (MinEcon).

Positive institutional change can be seen through the reorganization of the State Informatics Agency into the Estonian Information Systems Authority (EISA) in 2011, an agency under MinEcon, which is mandated to deal with both development of e-society services and cybersecurity. More specifically, EISA's responsibilities lie in running the national CERT, developing procedures for CIIP, and exercising state control over CII of critical service providers.

Uncharacteristic of the agency's responsibilities, EISA's Statute also includes the role of cybersecurity policy development[56]. This is a direct effect of the NPM legacy of a decentralized thin state where the financial and personnel resources have been cut drastically, and with overall austerity measures the institutional capacity could not be re-developed on a ministerial level. Instead, it was delegated to a state-run agency. A further positive change can be seen in 2012. With the passing of the revised Defence League Act, the roles and responsibilities of the Cyber Defence League were finally legally set. Unfortunately in other areas, such as cyberdefence or the fight against cybercrime, institutional change is yet to achieve the same level as the results of the agencies. Thus, Estonia faces a situation where cybersecurity presents government agencies with a multitude of problems that are still characteristic of thin NPM driven states.

As stated, the exception to this rule is the institutional change in MinEcon, to foster the need for growing government support towards the growth of the information society. To this end, it is clear that the Estonian government is willing to develop new organizational structures and invest in people, as well as,

[53] | Op. cited Fisher, p. 19.
[54] | Op. cited Magretts, p. 5.

[55] | Kaska K. et al., Developments in the Legislative, Policy and Organisational Landscapes in Estonia Since 2007, [in] Tikk E., Talihärm A. (ed), International Cyber Security Legal & Policy Proceedings, CCD COE 2010, [online] www.ccdcoe.org, (access: 10.05.2012)
[56] | Ibid

allocate significant resources. However, the underlying difference, that is the basis for this decision, lies in the positive economic aspects of development of the information society in comparison to the seemingly negative attributes concerning cybersecurity.

In terms of cybersecurity policy and governance, the empirical study proved overall successful at testing the assumptions outlined in the introduction. The 2007 cyberattacks showed the vulnerability of the society and the dependence on ICT. The events proved that cyber means can be effectively used to exert societal anti-government pressure and seriously hamper a variety of information systems dependent services.

Furthermore, as such threats persist; one-time response measures in national emergency resolution are insufficient and a broad approach to securitizing cyber is necessary. Most cyberthreats were shown to be directed at private entities (businesses and individuals). Thus, governance instruments should create the basis for safer information exchange, provide aid in technical cybersecurity crisis management, and ensure modern legal instruments so businesses and individuals can be protected in the cyber realm as they are protected in their physical lives.

> “ One-time response measures in national emergency resolution are insufficient and a broad approach to securitizing cyber is necessary.

Irrespective of some policy watershed since the securitization of cyber in 2007, overall, Estonian cybersecurity policy and legislative improvements have been considerable. Cybersecurity policy may not meet all the Fisher policy criteria[57], and it certainly does not account for the lack of people management and insufficient organizational aspects of cybersecurity governance, but the shortfalls can be attributed to the reactionary nature of the emergence of the cybersecurity governance paradigm. As outlined, some policy gaps could be filled by regulatory change governing the “organization of the state” that would mean the revision of statutes of ministries and other government agencies and inclusion of cybersecurity tasks[58]. Failure in this is most prominent and detrimental to the success of Estonian cybersecurity policy implementation and depicts the general inability to let go of the lean organisational structures favoured in NPM.

Understandably, it is difficult to create a viable policy on something that is not a subject in itself but the means for executing most of the daily tasks and activities that people in our societies perform. If one does not understand the subject matter, it is impossible to govern something that has not been defined. The key is to distance oneself from the fact that cybersecurity governance touches upon human activities in relation to information systems. In fact, it is the human action, the people’s rights, obligations, penalties etc. that should be enforceable through effective governance.

4. The New Paradigm – Cybersecurity Governance

The success in tackling cybersecurity issues in the future lies in a twofold approach, primarily based on the reorganization and development of the theoretical base into more appropriate for the needs of information society.

The instruments for tackling governance gaps include: selective institutionalisation, public sector education and task specification, and securitization of (e-) service development /lifecycle.

Selective institutionalism is a direct recommendation based on the findings of the case study of the Estonian public sector capability to tackle cybersecurity policy creation and adoption gaps and the necessity for cybersecurity, where the risks stemming from disregarding the security agenda by the government, would lead to significant negative impact on societal well-being and security as members of the information society. In securitized agendas, it is unacceptable that government agencies have no specified tasks related to that agenda, in this case cybersecurity.

[58] | Op. cited Kaska et al.

Furthermore, it is unacceptable that the highest policy setting agencies have no cybersecurity expertise, or that the experts responsible for policy on cyber elements of the respective ministries are double-hatted, performing a variety of other tasks. To this end, a single strong lead agency should be appointed, reassigned, or developed to handle all co-ordination and policy lead functions, as well as, oversight of policy adoption by other agencies.

The element of smart engagement indicates the growing need for governments to engage in co-operation with the private sector. However, in this instance it is not outsourcing as presented in NPM. In fact, by this ideological change to governance, governments should use private sector/service provider information on the provision of services, the private sector data on cyberthreats, and the correlation of threats to the segments of services with highest dependence/use by the end-user on a partnership basis, allowing for policies to be set based on the most recent and most impacting threat vectors and perception.

Public sector expertise building directly follows selective institutionalism, as establishing central government organizations to deal with cybersecurity policy creation and implementation, is inadequate without a specifically trained staff.

Securitizing of (e-)service development/lifecycle planning is a natural process supporting the proposed digitization and creation of universal online services, as proposed in DEG. Securitizing e-services development ensures that the positive aspects of the Internet and e-services, as well as the ambivalence of technology dependence and associated cybersecurity risks are accounted. Moreover, this instrument would ensure that cybersecurity risk would be considered already at the planning phase of service development and emergency planning.

Cybersecurity is, by definition, a phenomenon best described by its interdependence. Thus, joint, smart, and sustainable solutions must be the goals of governments and not of tech-heavy companies alone. Cybersecurity should no longer be viewed as unnecessary investments, but the means to ensure the widest level of societal wellbeing and functioning. ■

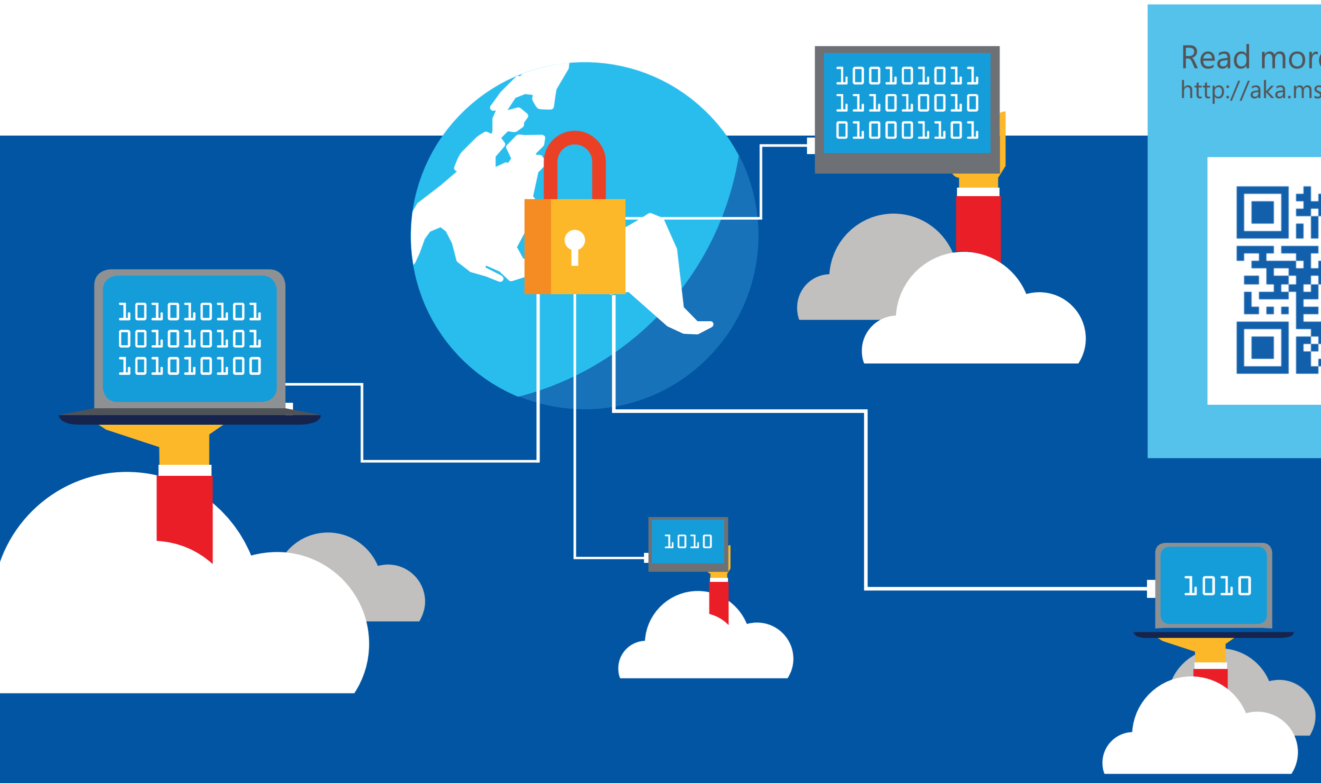
Microsoft

Cyberspace Needs Norms

Cyber conflict and cyberwar are not just theoretical but actual possibilities that need to be considered and addressed. Information and communications technology creates benefits for states and their citizens alike, but technologies can and are being exploited by a variety of government actors with differing motivations and means. For nearly two decades, the cybersecurity community has warned of the increasing number and sophistication of cyber attacks. But now, cyberspace is being operationalized by some nation states as a domain for conflict, dramatically escalating the threat. In this shared and tightly integrated domain, any escalation of hostilities could result in unintended and even catastrophic consequences.

Reducing this risk requires an inclusive global dialogue on the development of norms that advance cybersecurity.

Microsoft proposes six norms to limit conflict in cyberspace.



Read more at
http://aka.ms/cybernorms

OPINION

CYBERSECURITY IS A TEAM SPORT

PIOTR PUCZYŃSKI

Piotr Puczyński is the Vice President of the Management Board at Bank Gospodarstwa Krajowego. During his 25 year professional career he dealt mainly with implementation of new solutions, changes, and innovation in the financial sector, working with Bank Millennium, Bank BWE, Bank NORD L/B, and the PZU Group. In 2009-2013 working with Microsoft Polska he cooperated with the DNB, BOŚ, ING Bank Śląski, and BRE Bank. In 2013-2014, he held a managerial position at Poczta Polska.

Signing the "Executive order on sharing cybersecurity threat information", President Barack Obama said: "The cyber world is the wild, wild west..."

I wish it were that simple, one might say. Unfortunately the times of a lone sheriff duelling "the bad guy" in the middle of a town are over. It is more like "Ghostbusters", as our enemies appear and disappear like ghosts. They present a common threat to everyone: consumers, states, businesses, economies, trades, citizens, etc. But while we acknowledge this threat, we are still looking for a "High Noon" scenario. Verbally, we agree more and more that cooperation is needed to be able to stand against "the enemy". But it seems that there are still many different points of views and different interests. The Snowden case brought into the picture the big issue of keeping the balance between national security and information privacy.

So everybody agrees that there is a need for sharing information to protect our countries, businesses, and private data from cyberattacks. But on the other hand we are not willing to agree that "someone is going to watch me". We are more and more afraid of losing our privacy or our competitive advantage.

It seems that we are more divided than ever. There is a split at the interstate relationship level. We are dealing with an enemy who has no problem with crossing any borders. But we as "the good guys" have to deal with legislation systems that vary from country to country. Every investigation process is difficult and time-consuming. Furthermore, potential sentences for cybercrime also vary between countries. So even if you are caught, but "properly" located, the punishment might be e.g. 6 month suspended prison sentence. Compared with a potential "reward" – not much of a risk.

Furthermore, the potential of cyberspace was also noticed by military strategists. It seems that you can harm your enemy more in cyberspace than anywhere else. What makes it more attractive – you can stay anonymous during such an attack. You launch a "regular" missile and within minutes everybody knows you did it. You attack some important infrastructure and cause a blackout in the targeted country - it takes a lot of time for you to become a suspect. So we can see that at the international level it is hard to secure any agreement.

There is also a split between private and public entities. In principle, cooperation of those two sectors is a challenge. It is also regulated differently in different countries. The basic principle of capitalism is "free economy", so any intervention of any state is perceived as a threat to the freedom of doing business. The basic argument is that private entities are running their businesses at their own risk, so they need to take care of their own security. But even many large companies may not be able to do this on their own. The case of the cyberattack on Sony Pictures Entertainment shows that no one is safe. Especially that in the Sony case we probably saw an attack launched by a country against a private enterprise. That shows that there is a need for cooperation in this respect, but yet there is no mechanism developed for it. What makes the case even more complicated is the fact that every such example of cooperation might have a negative impact on the opinion of customers. That is because we also face a dispute between the state (any state) and its citizens about data privacy. No matter how democratic our countries are, we are not happy to know that there is always someone able to look into our private lives. And this is true whether it is a company providing us with any kind of products (e.g. a supermarket connected with our fridge and delivering goods without our participation) or service (e.g. banks).

> “ We also face a dispute between the state, or any other state and its citizens about data privacy.

This discussion started at its full potential after September 11, 2001 with the “war against terror”, but are we any closer to a conclusion? Are we OK if my state, or any other state browses my private emails to spot any suspicious words? Regardless of any threats, any company that has an official agreement with the state to exchange information about its customers might get into serious trouble. We, as customers, want to have the full right to decide about our personal and private data. It is important to remember what happened with an attempt to get into agreement on protection of Intellectual Property. The whole ACTA issue triggered a sometimes quite violent discussion. It seems that a considerable number of people treat cyberspace as an unregulated area. After many years of negotiations the presented project ended up being treated as an attack on the freedom of the Internet. I do not think that the general perception of cyberspace and its “freedom” has changed since. In that sense it is still a “...wild, wild West”.

Last but not least, commercial enterprises seem to be very little involved in the battle against cybercrime. „Competitive advantage” seems to be the main worry. There is a concept that any cyberattack on our competition helps to strengthen our market position. This leads to a strong resistance to sharing any information about cyberattacks. On one hand, everybody agrees that information sharing is important in protecting organizations against cybercrime, but on the other, everybody wants to be a “passive” participant – using information from others, rather than giving away any information about their own experience. The question is whether for example a large scale cyberattack on a particular bank does not decrease the level of confidence in the whole banking sector? If the answer is “yes”, then from the competitive advantage point of view, when our competitor is having trouble, we are winning a battle but losing the war.

To summarize, if we look at the “good guys” front, we say that we all want to cooperate and fight against cybercrime. But if we look a little deeper under the surface we can see that there are still many issues with higher priorities than the battle against cybercrime. And if this battle is a team sport, we have no chance of winning it.

What can be done? Where can we go from here? I can see two levels of activity. A global and a local (national) one. On the global level, I would start from a redefinition of cyberspace. In principle, this is simple: “„the notional environment in which communication over computer networks occurs” (Oxford Dictionaries). But searching further one can notice that we still have a problem with a proper definition of cyberspace. It is becoming more and more complex and every day brings new aspects and examples that force us to change the definition. On the NATO Cooperative Cyber Defence Centre of Excellence main webpage we can find more than 20 different definitions from many countries. Furthermore – there is a general remark at the top of the glossary: “There are no common definitions for Cyber terms - they are understood to mean different things by different nations/organizations, despite prevalence in mainstream media and in national and international organizational statements.” This is not a good start for creating a common international jurisdiction. So we must agree on basic principles such as the definition of what we are talking about.

The second major step might be to start treating cyberspace the way we treat outer space, with all the consequences for any aspect of international law. Taking a view that cyberspace is not located on a particular server in a particular country with local jurisdiction, but instead constitutes a different dimension, opens up a set of new possibilities for discussing and developing a policy framework e.g. for cross-border cyber-investigation.

In the meantime, we should do what we can in our local markets. There is still a lot to be done within the current environment. Let us look at the banking system, which is my home ground. With increasing numbers of customers using modern channels of communication, there is an obvious rise of cybercrime risk. Before the era of mobile banking, there was much better control over communication with consumers. If anything like a cyberattack happened, it was possible to keep it low. The bank immediately paid compensation to the customer and there was no need to talk too much about it.

Nowadays, as mobile devices have become more open and hackers are smarter, the number of such incidents is rapidly growing. The potential cost of paying compensation to all customers affected by cyberattacks (regardless of the determination whether it was the bank's fault or not) is becoming too high. So we are facing the issue of communicating to customers that there is a risk of losing money which the bank is not going to cover. It is a good test to see whether there is a chance to reach an Agreement about a common policy within the banking sector and within one country (Poland). Do we know how to inform our customers that not everything is as safe as they think? How not to lose the trust of our customers? Can we solve this issue not in the "competitive" mode, but in a "cooperative" mode? Can we do it as a sector without any exceptions? All of this seems to be a challenge that can be overcome without any global decisions or change of the legislation system. And as long as we can do it, we can show some ability to work as a team.

Another example, again from the banking sector, also shows that to become more secure we must cooperate and be ready to make compromises. If we look at the process of stealing money from any bank account, there is a scenario similar to a "traditional" robbery. One needs to get into the bank, take the money and... get out of the bank. The difference is that as the last phase in "traditional" crime seems to be difficult, getting out of the bank in the virtual world is relatively easy. This is mostly due to the trend to speed up the process of payment for the sake of customer comfort. There is an option in Poland to transfer money "online" (SORBNET) between banks to an account which is opened automatically in the bank of the beneficiary, just for the sake of this particular payment. This is a very simple route to get out of the bank with stolen money.

> “ To become more secure we must cooperate and be ready to make compromises.

To keep our customers' money safer, we need to take care of security at each phase of the payment, but as long as we keep money within the banking sector, we have the ability to track it down and secure it. One of the possible actions we might take is to agree among banks not to allow anybody to open an account automatically just to receive payment. We probably should also put some restrictions on SORBNET payments. Generally, we should work together to keep stolen money in the system. Can we do it? Can we stop competing and start cooperating in this particular case?

To summarize, cyberspace takes our life to a different dimension. We already know that rules governing two dimensional space apply in 3D. But as the 3D world is different – we need to add new rules, so that our 3D world is better described and understood. I would take a similar approach to cyberspace – we cannot simply apply rules from our "real" world to the new space. We must look much further.

Finally, we must not hope that a lone sheriff is going to come and save us. We must start cooperating at every level. There is an urgent need for education among consumers, but also among corporate managers, public sector workers, and members of governments that there is a real threat. A threat that obviously is not going to stop us from exploring possibilities of this new realm, but which must be taken into account while we are harvesting new fields in cyberspace. And as we enjoy cooperation in doing business in cyberspace, we must get together as a good team, and win the game on securing this new land of opportunity. ■

POLICY REVIEW

EUROPEAN CYBER FOREIGN AND SECURITY POLICY THROUGH DIGITAL INTEGRATION[1]

DR ANNEGRET BENDIEK

Dr Annegret Bendiek is Senior Associate in the EU and Europe Division of the German Institute for International and Security Affairs (SWP) and Head of the SWP project on "The challenges of digitalization for German Cyber Foreign and Security Policy". This article has been written in cooperation with Tobias Metzger, M.A. and Christoph Berlich, M.A., members of the project team at the Stiftung Wissenschaft und Politik.

Digital information systems, above all the Internet, play a central role in the free movement of goods, services, and people across borders. Legislation at all levels struggles to keep pace with rapid technological advances, leaving many areas inadequately regulated. Yet legal security in dealing with technology and lasting public confidence in its reliability are crucial to economic development. For its current five-year term, the European Commission estimates that creating an interconnected digital single market could create additional growth of up to €250 billion[2].

Following the concept of negative and positive integration[3] there are two main options for state (de-) regulation in response to an expansion of economic space beyond national borders. Negative integration removes obstacles to competition and free trade (such as tariffs). This has a market-creating effect. Positive integration measures aim to correct market outcomes and overcome market failure. This requires economic policy coordination and regulatory powers at the EU level. Therefore, digital integration should – analogously to previous non-digital economic integration – be understood as the expansion of a unified societal space, which is subject to shared rules and which is characterised by the removal of institutional barriers between EU member states. Fundamentally, market regulation happens at multiple levels: global standards must be set in international forums, data protection should be harmonised at the EU level, while prosecution of cybercrime is mostly done at the national level (if necessary coordinated EU-wide). Digital regulation should, therefore, be understood as a multi-layered

[1] | An earlier version of this article has been publishes as an SWP Comments.

[2] | European Commission, Digital Agenda Review: Frequently Asked Questions, 2012 [online] http://europa.eu/rapid/press-release_MEMO-12-1000_en.htm (access: 16.6.2015). Castells M., Communication Power, Oxford University Press, Oxford 2009, p. 418.

[3] | Scharpf F. W., Regieren in Europa. Effektiv und demokratisch?, Köln 1999

structure. The existence of the single market makes the Union not only an important locus of regulation, but also a strong economic actor with the global ambition of digital assertiveness. In the past, establishing standards such as MP3, SMS, and Compact Disk in Europe has proven effective in compelling non-European market participants to join. As the experience of Airbus has demonstrated, and the satellite navigation system Galileo might, the EU framework can enable state and non-state actors to influence global standard-setting to an extent denied to individual states and private corporations.

Challenges of the Digital Single Market

The challenges associated with creating a digital single market can be illustrated by the virtual path of an e-mail. Which 1) hardware and software is used to write the e-mail, via which 2) Internet routing infrastructures is it transmitted, on whose 3) data servers and cloud services is it saved, with which 4) techniques is it encrypted there, and by which 5) data protection and competition regulations is it protected? These steps along the digital path demonstrate the need for regulation and reveal why the European Union is the appropriate level at which this should occur:

> “ The existence of the single market makes the Union not only an important locus of regulation, but also a strong economic actor with the global ambition of digital assertiveness.

Firstly, Europe, apart from a handful of exceptions such as SAP and Alcatel-Lucent, ceases to be a relevant actor in the software and hardware sectors. The European industry’s dependency on US and Chinese components makes a completely independent European market inconceivable. Many industries, such as that of search engine providers, are currently dominated by quasi-monopolists: Microsoft, Google, Cisco, and Huawei. The leading PC manufacturers include Apple, Dell, HP (all USA), MSI, ASUS, Acer (all Taiwan), Samsung (South Korea), Lenovo (China), and Toshiba (Japan). Some of these are also among the world’s leading smartphone manufacturers, alongside Huawei (China) and LG (South Korea). Hardware components for home networks originate largely from Cisco (USA) or Huawei (China), while HP leads Dell and IBM in server hardware for data centres. The market share of European competitors (Siemens, Nokia) has shrunk significantly, leaving a de facto US-Asian duopoly. Secondly, Europe needs a reliable communication network operated and administered in the public interest. Individual interests should only be provided space where they align with the general interest. Precisely the opposite is the case in Europe today. The Internet consists of national networks, each with its own set of controllers, respectively pursuing particular interests. In theory, the Internet comprises the networks of various Internet service providers (ISPs), which are joined at neutral points (Internet exchange points) to create the network of networks. In practice, the notion of neutrality is questionable. DE-CIX is the largest of the worldwide 321 Internet exchange points and belongs to the Association of the German Internet Industry (eco). DE-CIX is run in a manner that grants access to the German intelligence service BND, thus compromising the data of primarily non-German entities[4]. One may doubt whether this procedure safeguards European interests.

Thirdly, diverse new challenges arise with respect to cloud computing and distributed data processing and storage. The problem for positive regulation of European data and consumer protection is that the legal and economic spaces are not necessarily identical. Where data and access requests are outside the reach of European law enforcement, European legislation is toothless. The danger of major data theft from cloud platforms lurks above all when servers are located outside of Europe. Furthermore, terms of business that grant access rights to third parties can have unforeseen consequences. Not only do US providers have to hand over data stored on European servers when requested (see the case of Microsoft Ireland versus the US Department of Justice[5]), but European firms operating in the United States are also subject to the same obligation.

Fourthly, the digitalisation of communication has hollowed out the right to privacy. As the Snowden

[4] | Biselli A., Betreiber des Internetknoten DE-CIX will gegen den BND klagen, 2015 [online] https://netzpolitik.org/2015/betreiber-des-internetknoten-de-cix-will-gegen-den-bnd-klagen/ (access: 31.08.2015)

revelations demonstrate, state security agencies can access and analyse unencrypted e-mails whenever they wish. Yet privacy and liberty are fundamental conditions for the market itself and therefore require protection. In liberal societies the right to privacy is also constitutive, for without privacy there can be no liberty. The endangerment of data privacy and consequently social liberty calls for a European response. Because telecommunications infrastructure is in private ownership and networks transcend national borders, the emphasis is currently on improving encryption methods. However, encryption technologies must come without any hidden access options (back doors) demanded for investigation purposes not only by the Chinese government but also by its US American and British counterparts. A great deal of information can also be gleaned from encrypted e-mails. The metadata – so to speak the envelope containing the message – reveals who is in contact with whom, when and how often, and even the subject line of the message.

Fifthly, quasi-monopolies of major corporations are fundamentally problematic. Cartels and other forms of market domination lead to higher prices, inferior products, and grave deviations from the ideal of the free market. Although merger controls do exist, European competition law in many cases does not respond with sanctions until market domination has actually led to abuses. Nonetheless, we are seeing extensive debate on whether US technology giant Google occupies a market-dominating position in Europe.. In November 2010, then EU Competition Commissioner Joaquín Almunia opened a case against Google, which his successor Margrethe Vestager has now revived after collating extensive evidence that Google's search results systematically favour its own services over those of its rivals. The Competition Commissioner is also taking action against several states that may have granted corporations such as Amazon and Apple advantages through tax rulings. If individual companies benefit at the cost of their rivals, this constitutes a violation of competition law.

Deepening Digital Integration

Historically, regulatory challenges of the kind illustrated using the virtual path of an email have often contributed to ambitious leaps in European integration. The most striking example is the creation of the internal market through the Single European Act in 1987[6]. In order to deepen digital integration, Andrus Ansip, Vice President of the European Commission for the Digital Single Market, and Günther Oettinger, Commissioner for the Digital Economy and Society since November 2014, are therefore pushing hard for the establishment of a digital single market. The objective is to expand the advantages of the European internal market to the digital sphere. According to the Commission, we will only benefit from the technical innovations associated with big data, cloud computing, and the Internet of Things, if attempts at digital sovereignty are overcome in favour of a European harmonisation of national markets. The April 2014 ruling of the European Court of Justice, overturning the Data Retention Directive and demanding greater data protection and security on the basis of European law, can be considered an instigator for initiatives to realise the digital single market[7]. The ruling sets legal limits on the storage of information of EU citizens in third countries and provides economic incentives for establishing a European network infrastructure.

The Strategy for a Digital Single Market

The Digital Single Market Strategy published by the European Commission at the beginning of June 2015 comprises sixteen measures to be implemented by the end of 2016[8]. It is based on three pillars: 1) better access to digital goods and services for consumers and businesses across Europe; 2) the creation of infrastructure for digital networks and services, and 3) the exploitation of growth potentials of the digital economy.

By virtue of market-creating measures defined in the first pillar, companies in the digital single market

[5] Please insert the source here: Beiersmann S., Microsoft wehrt sich erneut gegen Zugriff von US-Behörden auf in Irland gespeicherte Daten, 2014 [online] http://www.zdnet.de/88213556/microsoft-wehrt-sich-erneut-gegen-zugriff-von-us-behoerden-auf-irland--gespeicherte-daten/ (access: 31.08.2015)

[6] EUR-Lex, The Single European Act, [online] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:xy0027 (access: 31.08.2015)

[7] Court of Justice of the European Union, The Court of Justice declares the Data Retention Directive to be invalid, 2014 [online] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf (access: 31.08.2015)

[8] 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 Single Market Strategy for Europe, 2015 [online] http://ec.europa.eu/priorities/digital-single-market/docs/dsm--communication_en.pdf (access: 31.08.2015)

should experience no (or only minimal) obstacles compared to national commerce (negative integration). To this end, contract law and VAT rules are to be harmonised and cross-border data delivery services improved. The strategy also has the goal of ending access restrictions (geo-blocking), for example by standardising copyright law. The Commission wishes to reduce barriers to e-commerce, harmonise tax rules, investigate the market power of online platforms such as search engines and social networks, and reform the legal framework for audio-visual media.

As part of the second pillar, the Commission proposes new rules (positive integration). The planned NIS Directive[9] will make operators of critical infrastructure liable for failures. Apart from having to ensure better IT security, providers of services such as trading platforms, payment systems, social networks, search engines, and data clouds will be obliged to report serious cyberattacks and will have to implement appropriate safeguards in line with the planned EU rules. The rights of the end user, as the weakest link in the chain, will also be strengthened by compelling providers to report security violations and loss of integrity (data falsification). Technical norms are to be harmonised and trustworthy cloud services certified. The Commission will also review the indemnifications for providers affected by the Electronic Commerce Directive and harmonise procedures for removing illegal content from the Internet (terrorist propaganda, child pornography, copyright violations). An extensive reform of copyright law is currently under discussion in the European Parliament.

The third pillar is about both expanding the European digital economy and about supporting the increasing use of digital technology in conventional industry. Medium-sized businesses and start-ups are to be supported through easier access to investment capital, and the legal regulation of portability, interoperability, and standardisation is to be improved with regard to cloud computing and big data solutions. The main thrust of the EU regulation is to prevent confidential data getting into the wrong hands on account of inadequate security or a defective legal framework.

Restrictive laws on data location and encryption methods are to be harmonised so that all European market participants are treated equally in all respects. It is important to remember that data routing between places outside the United States, for example communication between Estonia and Italy, may still pass through US servers. The feared consequences for data protection lend weight to calls for restricting routing to the Schengen area. However, this is problematic for economic reasons and since it risks decreasing technical reliability. The US Trade Representative (USTR) regards it as a violation of international trade agreements – even though similar arrangements also exist in the United States.

A more convincing proposal comes from the European Network and Information Security Agency (ENISA). It contains possibilities for end-to-end encryption for various applications (securing data when sending and receiving as well as in transit). Methods for disguising metadata are also considered, for example using virtual private networks or onion routing to encrypt an e-mail multiple times. The encryption layers are then placed like envelopes around the actual message, with each party involved permitted access only to the information it requires to forward the message.

The EU Directive on Network and Information Security

It is widely understood that due to the connectedness of today's societies, governments must ensure the protection of core "critical" infrastructure (CRITIS), include the health care, food and water sectors, financial services, transportation, energy supply, and public administration. As many infrastructural elements are owned by the private sector, governments face the significant challenge of having to establish and strengthen previously unusual cooperation and information exchange between public and private as well as civilian and military bodies. Unlike the very different approach of the US administration – with its voluntary platform for information exchange (NIST Cybersecurity Framework) – the EU introduces mandatory reporting and imposes severe fines for infringements in its ongoing legislative procedure for a Directive on

[9] | 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 Single Market Strategy for Europe, 2015 [online] http://ec.europa.eu/priorities/digital-single-market/docs/dsm--communication_en.pdf (access: 31.08.2015)

[10] | NIST, National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, 2014 [online] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (access: 31.08.2015)

Network and Information Security (short: NIS Directive)[10]. The NIS Directive will make operators of such critical infrastructure liable for failures and it demands for “operators providing essential services” and “key Internet enablers” to improve their risk management.

It also calls for member states to adopt national cybersecurity strategies, and to staff and finance computer emergency response teams (CERT or CSIRT).

Apart from having to ensure appropriate IT security safeguards in line with the planned EU rules, providers of services such as trading platforms, payment systems, social networks, search engines, and data clouds will also be obliged to report serious cyberattacks to national authorities. Furthermore, the rights of the end user, as the weakest link in the chain, will be strengthened by compelling providers to report security violations and loss of integrity (data falsification). Technical norms are to be harmonised and trustworthy cloud services certified. While the formal negotiations of the “Trilogue” (European Commission, European Parliament, and Council of the European Union) have not started, there have been three informal Trilogue meetings, the last of which in April 2015. The NIS Directive is accompanied by the “NIS Platform”, installing cross-sectoral working groups to help implement the Directive’s measures[11].

In the meantime, Germany has adopted the EU’s first national IT Security law (IT Security Act, IT Sicherheitsgesetz)[12]. Similar to the draft of EU NIS Directive, it requires operators of critical infrastructure to ensure minimum standards of IT security and to report incidents to the Federal Ministry of the Interior’s IT security agency (BSI, Federal Office for Information Security). According to the law, the government may call on companies to fix known vulnerabilities in a timely manner and impose penalties for non-compliance. To allow for speedy adoption of the Act and to ensure its flexibility and long-term relevance, an additional decree is to be issued to define the sectors and companies to be included in the CRITIS definition.

> “ Governments face the significant challenge of having to establish and strengthen previously unusual cooperation and information exchange between public and private as well as civilian and military bodies.

Data Protection as Competitive Advantage

To counteract illegal exploitation of content and data on the Internet, copyright, data protection, and consumer rights are also to be refined at the national and European levels. The aim of the planned European General Data Protection Regulation (GDPR) is to enforce data protection in order to improve legal certainty for businesses in the internal market[13]. In June 2015, after more than three years of negotiations, the EU interior and justice ministers agreed on a joint position towards reform of data protection rules.

The proposal is now under discussion in the Trilogue between the European Council, Commission, and Parliament. The new GDPR is intended to come into force in 2018 to replace the Data Protection Directive of 1995. It proposes to compel businesses to implement strong default privacy settings in their technologies, enable class action suits over privacy violations, improve cooperation between national regulators, and create a harmonised oversight mechanism. Not least, sanctions in response to data protection violations are proposed. While the original draft of the European Commission sets these at two percent of the company’s global turnover, the European Parliament calls for the fine to be set at five percent of annual turnover and at least €100 million[14].

The “right to be forgotten”, which the Spaniard Mario Costeja González won from Google in the European Court of Justice ruling of 13 May 2014 and which has transformed Europe’s digital economy, is a central point in the GDPR[15].

[11] | SA, NIS Platform, [online] https://resilience.enisa.europa.eu/nis-platform (access: 31.08.2015)

[12] | Bundestag, Bundestag beschließt das IT-Sicherheitsgesetz, 2015 [online] https://www.bundestag.de/dokumente/textarchiv/2015/kw24_de_it_sicherheit/377026 (access: 31.08.2015)

[13] | European Parliament, Personal data protection: processing and free movement of data (General Data Protection Regulation), 2012, [online] http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011%28COD%29#basicInformation (access: 31.08.2015)

[14] | Albrecht, J. P., EU General Data Protection Regulation State of play and 10 main issues, 2015 [online] https://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf (access: 31.08.2015)

Teisch R., Progress on Data Protection in the European Union, 2015 [online] http://www.jdsupra.com/legalnews/progress-on-data-protection-in-the-78103/ (access: 31.08.2015)

[15] | European Commission, Factsheet on the “Right to be Forgotten” ruling, [online] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (access: 31.08.2015)

The ruling states that search engines must observe valid data protection directives and cannot fall back on American law even if the parent company is headquartered in the United States and its data are processed there. Every EU citizen now has the right to demand for the search engines to delete their personal information. Google alone, according to its own figures, had received 309,666 deletion requests by 31 August 2015, 41.5 percent of which had been fulfilled[16].

Under Article 23 (1) of the GDPR, data protection must in the future be integrated directly into processes, systems, and products. Sensitive data from EU citizens may only be passed to foreign security agencies under the terms of a judicial assistance agreement. Under current law, it is forbidden to transfer personal data from member states to countries that do not possess data protection comparable to European law[17]. This is an important issue, because the European constitutional understanding diverges significantly from the American one. In the United States the focus is not on the protection of human dignity, but on freedom in the sense of liberty as a civil right of the individual, who wishes to be "free of legal regulations". But the new GDPR and the proposed directive on personal data protection in law enforcement[18] are aimed at implementing legal guarantees for EU citizens in the judicial assistance system. The data protection reform package will therefore have repercussions on all new bilateral agreements with the United States on data transfer in the areas of security and economy. This includes, among others, the exchange of personal data, the data protection umbrella agreement, the bilateral mutual legal assistance agreement, and the exchange of airline passenger data.

Europe in the Digital World

The European regulatory system is not restricted to the internal market, but also has a global dimension. The European information and communications sector is closely interconnected with other markets. In order to take account of the reciprocal dependencies of European and global standards and rules, the European Commission and individual member states have become active in international bodies on the central issues of Internet Governance and cybersecurity. For this reason, digital integration also comprises a foreign policy dimension affecting not only the expansion of the digital internal market beyond national borders but also the member states' cyber foreign and security policy. Accordingly, the European Council conclusions on Internet Governance of November 2014 and on Cyber Diplomacy of February 2015 call for a "multi--stakeholder approach", including representatives of business, the technical community, science and civil society, as well as governments[19]. Furthermore, they demand close cyber diplomacy with the United States, for example in the Group of Governmental Experts (GGE) at the UN level.

In the relevant documents on European Cybersecurity of February 2013 and on Internet Governance of February 2014, the European Union argues that freedom, security, and stability are vital for the long--term maintenance of cyberspace[20].

> " Digital integration also comprises a foreign policy dimension affecting not only the expansion of the digital internal market beyond national borders but also the member states' cyber foreign and security policy.

Heise online, Mehr Datenschutz für Internet-Nutzer in Europa, 2015 [online] http://www.heise.de/newsticker/meldung/Mehr-Datenschutz-fuer-Internet-Nutzer-in-Europa-2690164.html (access: 31.08.2015)

[16] | Google, European privacy requests for search removals, [online] http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en (access: 31.08.2015)

[17] | Europäische Gemeinschaften, RICHTLINIE 95/46/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 24 . Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener, 1995 [online] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046&from=de (access: 31.08.2015)

[18] | See more about guidelines for prosecution service: http://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-law-enforcement/

[19] | Council of the European Union, Council Conclusions on Internet Governance, 2014 [online] http://italia2014.eu/media/3769/council-conclusions-on-internet-governance.pdf (access: 31.08.2015)
Council of the European Union, Draft Council Conclusions on Cyber Diplomacy, 2015 [online] http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf (access: 31.08.2015)

[20] | European Commission, JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013b [online] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (access: 31.08.2015)
European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Internet Policy and Governance Europe's role in shaping the future of Internet Governance, 2014b [online], http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52014DC0072 (access: 31.08.2015)

Internet Governance refers to the development and application of shared principles, norms, and approaches in global communication. Since June 2011, the European Commission has been pursuing the objective of creating "a single, open, free, unfragmented network of networks, subject to the same laws and norms that apply in other areas of our day-to-day lives" (in EU terminology: COMPACT)[21]. In order to prevent state influence from eroding the multi-stakeholder approach, the European Union intends to strengthen the role of the Internet Governance Forum (IGF), the global multi-stakeholder forum, with 3,700 members from 144 countries (2014). The UN General Assembly will decide at the end of 2015 whether to continue the format. At the same time, the European Union is calling on the organisations managing the Internet to "internationalise". This primarily concerns ICANN (Internet Corporation for Assigned Names and Numbers), which is responsible for the stable functioning of the Internet, and its IANA department (Internet Assigned Numbers Authority), which assigns numbers and names on the Internet, above all IP addresses. The European Union wishes to prevent individual states or private interests from dominating the administration of Internet resources. Therein, the EU is (at least officially) at loggerheads with the United States, which plays a leading role in ICANN. The process of preparing improved accountability procedures, for example to challenge decisions of the ICANN Board, is ongoing. ICANN CEO Fadi Chehadé has already stated that it will not be possible to complete the hand-over of oversight of core Internet administrative functions by September 2015 as planned. Therefore, he said, ICANN will be extending its contracts with the US Department of Commerce[22].

Another arena of multi-stakeholder discussion was the NETmundial conference in 2014, where the focus was on human rights and the right to privacy on the Internet. As a result, a European, Joseph Cannataci from Malta, was appointed as the first UN Special Rapporteur on the Right to Privacy by the UN's Human Rights Council in July 2015[23]. Moreover, at the initiative of the World Economic Forum (WEF), the Brazilian Internet Steering Committee (CGI) and ICANN, the so-called NETmundial Initiative (NMI) was launched in January 2015[24]. However, with European participants criticising its composition and lack of distance to the IGF, it has yet to establish a place for itself in the Internet governance ecosystem.

In an open letter of April 2015, Federica Mogherini, High Representative of the European Union for Foreign Affairs and Security Policy, and Dutch Foreign Minister Bert Koenders lay out the European Union's lowest common denominators. They point out the necessity to hold states responsible for attacks originating from their own national cyberspace and emphasise that inadequate protection of central infrastructure represents a threat not only to national but also international security[25].

This lowest common denominator was promoted by five EU member states in the fourth round of the UN Group of Governmental Experts (GGE) on cybersecurity (altogether representing twenty governments: Antigua and Barbuda, Belarus, Brazil [chair], China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russia, Spain, United Kingdom, and USA). Diplomats in the GGE analyse security risks in cyberspace and develop confidence building measures (CBM) as well as starting points for cooperation. The last session of the fourth round was held in New York in late June 2015; its final report has yet to be adopted by the UN General Assembly. The concrete application of international law to cyberspace continues to be a source of conflict (UNODA, n.a.). Incompatible interpretations of information security make a substantive subject-matter discussion at the UN level almost impossible. Contested issues include the scope of issues to be discussed, differing threat perceptions, and the envisioned role of the UN and governments vis-à-vis private-sector and civil society actors. While there is broad agreement that states must be held responsible for their behaviour in cyberspace, Germany and the United States

[21] | European Commission, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. Internet Policy and Governance Europe's role in shaping the future of Internet Governance (COM/2014/072), 2014 [online] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52014DC0072&from=EN (access: 31.08.2015)

[22] | Elder J., U.S. Delays Giving Up Oversight of Internet Administrator Icann, 2015 [online] http://www.wsj.com/articles/u-s-delays-giving-up-oversight-of-internet-administrator-icann-1439851721 (access: 31.08.2015)

[23] | Ermert M., Datenschutzfähnchen im Wind, 2015 [online] http://www.zeit.de/digital/datenschutz/2015-07/datenschutz-un-cannataci (access: 31.08.2015)

[24] | NETmundial Initiative, NETmundial Initiative, [online] https://www.netmundial.org/ (access: 31.08.2015)

[25] | Koenders B., Mogherini F., Cyber space needs stronger rule of law, 2015 [online] https://euobserver.com/opinion/128342 (access: 31.08.2015)

regard current international (humanitarian) law as the sufficient legal starting point for cyberspace, while Russia, China, and other states demand the development of specific international law for cyberspace. The G-77 states are above all interested in discussing the topic of cybersecurity in an open working group or carrying it into the Geneva Conference on Disarmament. The European Union does not operate as a monolithic bloc at the UN level, but coordination exists between Germany, France, and the United Kingdom. This coordination also includes other like-minded Western countries in the group. With Russia already calling for a fifth round of GGE discussions, we have reason to believe that the EU member states represented there will have to keep a stronger eye than ever on European interests[26].

Requirements for German Policymakers

Many regard the EU's overall digital strategy as without ambitions and incapable to advance Europe's digital assertiveness vis-à-vis the United States and China. Even large member states like Germany can exert global influence only in cooperation with EU institutions and other member states. The Friends of the Presidency Group on Cyber Issues (FoP Cyber) coordinates within Europe to support the respective EU Council Presidency, and should also expand its remit to international organisations[27]. The EU's digital assertiveness requires additional international flanking measures in order to stabilise the values of freedom and democracy in Europe and generate greater global traction. As part of the 2014 Digital Agenda, the German government has stated its intent to take "measures to regain technological sovereignty" and to create "a European area of trust"[28]. In the logic of negative and positive integration (Scharpf), technological sovereignty in the internal market would be legitimate only where it does not undermine significant achievements of social market economy and democracy. The internal market is based on fundamental trust in the forces of the free market and principles of openness and non-discrimination. Scepticism is therefore warranted towards the establishment of heavily subsidised national or European companies. State intervention is only appropriate where the market fails in providing important goods such as data security and privacy. Reciprocal global dependencies are not per se problematic, but become unacceptable when they undermine Europeans' ability to autonomously control their data and systems vis-à-vis illiberal governments. States that reject values such as the free market, democracy, and human freedom should be regarded as second-choice sources of strategically important resources for European communication infrastructure. Purchasing rare earths from Australia, for example, is more expensive, but avoids political double standards.

The case of Estonia offers an example of a successful digitalisation strategy. With only about 1.3 million inhabitants, the country is a pioneer of digitalisation in Europe. Its national e-ID infrastructure is used by more than 90 percent of its citizens. The digital ID card has a range of functions and can be used on the Internet wherever identity verification is required, for example for bank transactions or voting. Estonia operates largely without using Russian infrastructure and technology and has established a strong security network with eight international mirror servers in friendly states, including the United Kingdom, Germany, the United States, Canada, South Africa, and Japan. As far as electronic governance is concerned, small countries like Estonia are considerably further advanced than the big EU member states.
The further the European Union advances its digital integration in the form of European law, the more it will strengthen its digital assertiveness, both within Europe and internationally. The market location principle, a central instrument of the internal market, guarantees equal treatment of domestic and foreign businesses. Digital assertiveness depends crucially on the willingness of member states to expand the quantity and quality of European law. Only the European Union has the potential to forge a third way outside of the technological dominance of the United States and China, not individual member states. ■

[26] | Tikk-Ringas E., CYBER SECURITY PROCESS BRIEF: UN FIRST COMMITTEE 1998-2012, Genf 2012
UNODA, GGE Information Security. Developments in the field of information and telecommunications in the context of international security, [online] http://www.un.org/disarmament/topics/informationsecurity/ (access: 31.08.2015)

[27] | Friends of the Presidency, FRIENDS OF THE PRESIDENCY, 08/06/2015, 2015 [online] http://www.consilium.europa.eu/en/meetings/mpo/2015/6/friends-of-the-presidency-%28cyber-issues%29-%28238003%29/ (access: 31.08.2015)

[28] | BMWi, Federal Ministry for Economic Affairs and Energy, Digital Agenda, 2014 [online] http://www.bmwi.de/EN/Topics/Technology/digital-agenda.html (access: 31.08.2015)

EXATEL

people behind technology

Do you need help in designing a comprehensive system for IT security in your company or institution? Contact us!

Exatel SA ul. Perkuna 47, 04-164 Warszawa
tel. +48 22 340 66 60, fax: +48 22 340 66 66
e-mail: bok@exatel.pl, **www.exatel.pl**

Exatel - a provider of innovative services in the field of IT security

Exatel is the leading Polish telecommunications operator that provides modern ICT Solutions for medium and large enterprises and public administration. For over ten years, Exatel has been responsible for transmission speed and data security of customers in such industries as: banking, energy, telecommunications and others. Exatel is a part of the PGE Capital Group - the largest energy company in Poland.

We offer customized and technologically advanced solutions in the field of IT security:

✓ Anty DdoS
✓ Managed Firewall
✓ Audits/Penetration tests

We also offer:

✓ Lease of lines
✓ Data transmission
✓ Internet
✓ Wholesale voice services
✓ Communication
✓ Data Center
✓ IT security
✓ Intelligent media metering

INTERVIEW WITH ADAM PALMER

ADAM PALMER

Adam Palmer manages global cybersecurity policy and government affairs for FireEye. He is based in Munich, Germany. Adam began his career as a US Navy JAG Officer focusing on cybercrime prosecution. Most recently, Adam spent 2 years at the United Nations establishing the UN Global Programme against Cybercrime.

The EU is about to finalise a major new cybersecurity policy. How will this apply to Poland and what will be required?

The Network Information Security (NIS) Directive is expected to be finalised by the end of 2015 and will impose new strong security standards for many critical industry companies across Poland, as well as in the government. Most importantly, NIS will require these groups to adopt “state of the art security” controls to manage risk. This includes organizational and technical security measures to avoid interferences of availability, integrity, authenticity, and confidentiality of information technology systems. For cybersecurity, the NIS Directive requires the Polish government to develop and maintain:

- A national strategy;
- A national cooperation plan;
- A competent national coordination authority;
- Computer Emergency Response Team (CERT).

NIS also includes requirements for security audits and best efforts to report significant data breaches within 24 hours.

Although NIS provides approximately 2 years to implement these strategies, it is important that the Polish government and the included companies begin preparation now. Fines for non-compliance can be substantial and it will take time to implement these standards.

Germany recently became the first EU country to adopt an updated IT security law that requires a wide range of companies to adopt “state of the art security” similar to NIS. The German law mandates “state of the art” organizational and technical security measures to avoid interferences of availability, integrity, authenticity, and confidentiality of information technology systems. The law includes mandatory data breach reporting and regular audit requirements. I expect that Poland will be reviewing its current cybersecurity strategy and ensuring that it includes similar controls.

How is FireEye working with law enforcement to fight cybercrime?

In August 2015, FireEye signed a cooperation agreement with EUROPOL. This will allow for the exchange of knowledge and expertise on cybercrime, mainly in the areas of early detection of cybercrime threats and statistics on trends. Wil van Gemert, Deputy Director Operations at Europol said: „Law enforcement and private industry need to work together to effectively combat cybercrime, a growing problem on a global scale. The MoU with FireEye further strengthens our strategic cooperation with industry partners to target the criminals behind these crimes.” FireEye also works across Europe and globally with individual law enforcement groups to share information about advanced threats and support their efforts to fight cybercrime.

What do you recommend governments do as best practices for cybersecurity policy?

To promote economic growth and peaceful existence, it is critically important to protect commercial business, consumers, and the government infrastructure from advanced cyberthreats. This should include supporting initiatives that enable rapid and flexible acquisition of new cybersecurity capabilities that include not only traditional defence, but also capabilities to detect and mitigate threats by advanced cyber adversaries. It is critical to adopt measures that incorporate the best emerging practices for using signature-less behavioural detection techniques into a security framework that will put the government in a better position to identify and defend against sophisticated cybersecurity threats. To be effective, anti-malware solutions need to be intelligent enough to analyse network traffic and processes, rather than just compare bits of code to signatures. Dynamic analysis, as opposed to static signature-based comparisons, is critical to enable a product to detect and stop polymorphic malware on the wire as well as malware hosted on dynamic, fast-changing domains. In order to address these advanced threats, real-time, dynamic, and accurate analysis is critical. Rather than relying on signatures and lists, you must be able to dynamically recognise new attacks in real time, without requiring a prior knowledge of the vulnerability, exploit, or variant, and then prevent the system compromise and data theft.

While these are technical standards, it is important for policy to include these best practices. They are now basic security standards for any company or government agency. Technical solutions are only part of the answer. Government and private organizations can promote the proper risk management policy that encourages the right controls.

How does FireEye protect the right of innocent persons to privacy?

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against today's advanced cyberattacks. These highly sophisticated cyberattacks easily circumvent traditional signature-based defences, such as next-generation firewalls, IPS, anti-virus (AV), and gateways. The FireEye platform provides real-time, dynamic threat protection without the use of signatures to protect an organization.

A very small percentage of the overall network traffic is flagged as "unknown malware". This only occurs over non-encrypted customer channels. These channels are not expected to transport any sensitive or personal information. The likelihood of anything containing personally identifiable information (PII) is extremely low. Even with this very low probability, FireEye has put in controls to protect any personal information being distributed.

How has cybersecurity required a change in how the military approaches national defence?

Traditional IT security commonly uses defined criteria or patterns to detect threats. This is similar to digital fingerprints that identify threats based on known characteristics that have been seen in a prior attacks. However, this approach was fatally flawed. Advanced attackers can easily make changes to malware that alters the "digital fingerprint". Some organizations see hundreds or thousands of unique variabilities in malware designed to evade any pattern-based detection system. This has caused the need for a new approach focused on detecting threats based on behaviour and not on patterns or "signatures".

An even more serious and advanced attack is the use of a "zero day exploit". A zero day exploit is the security industry term for an unknown vulnerability in software or an IT system. These are unknown doors into systems that can be incredibly valuable for attackers to exploit. They are very difficult to detect and can cause large amounts of damage. Attackers may use a zero day exploit to launch a “zero day attack” that exploits this unknown vulnerability to enter and harm an organization.

The seriousness of zero day attacks was highlighted recently in a 2014 KPMG study of 20 large European multi-national companies finding that 93% of the organizations were breached, with 79% of the attackers stealing confidential data. Half of these attacks were successful by exploiting previously unknown “zero day” exploit vulnerabilities. By creating a unique “zero day” attack, an attack group can bypass any security that is based on defined patterns or “digital fingerprints”. This makes the detection and elimination of zero day vulnerabilities a primary concern for IT security managers.

What are the challenges for EU law enforcement investigating cybercrime?

The Challenges for EU law enforcement investigating cybercrime include:

- Putting the Suspect (if you have a suspect) at the Keyboard
- Size & Type of Data for Review
- Forensic Capability & Capacity
- Presenting Digital Evidence in Courts
- Victims: Identifying & Cooperation?
- Obtaining Evidence across National Borders Quickly

How does cybersecurity affect the national strategy of EU governments and impact Poland?

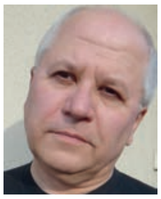
Looking at security incidents, from 2013 to 2014, there was a 41% jump in the number of cybersecurity incidents reported. What is at stake includes: jobs, Poland’s economy and reputation, and safety and privacy.

Governments must recognise that to effectively confront modern advanced threats, we must understand two things: that signature based defences offer protection against broad-scale attacks but do NOT stop targeted attacks, and the magnitude of damage a single targeted attack can cause to an organization. This understanding, in turn, has to lead to a change in policy to adequately account for this new advanced threat. ■

Questions by Natalia Płonka,
PR Manager of the Kosciuszko Institute

ANALYSIS

DATA AND CYBERSECURITY



DR JOZEF VYSKOČ

Jozef Vyskoč holds a RNDr. degree in mathematical informatics from the Comenius University in Bratislava, a MSc. degree in Computer Science from the University of Rochester, Rochester, NY, and a PhD degree in Management from the Faculty of Management, Comenius University in Bratislava. Owner of VaF, Ltd information security and privacy protection consultancy. Certified Information Systems Auditor (CISA) - the first CISA in the Slovak Republic. A member of programme committees of a number of international information security and privacy protection conferences.

While to begin small talk on cybersecurity is quite easy, to seriously address the problem of security of cyberspace on a national or international level, purely political declarations and awareness raising statements are insufficient and more concrete work has to be done. This is where the practical limits of our previous experience in information security are likely to show.

Cybersecurity differs from information security in that decisions, regulations, and other measures adopted, apply to a whole society or at least to a significant part of it and not only to one organization. That means a complex and diverse environment to be regulated, the existence of a variety of subjects along with their rights and legitimate interests that have to be respected, etc. This is what differs from the information security "playground" within a single organization. Let us face it – to manage cybersecurity on a national or international level, to make proper high-level decisions and implement them is a much more demanding task than to implement an information security management system in an organization. A call for solid fundamentals for such a task is then quite natural.

Know Yourself And You Will Win All Battles (Sun Tzu)

Governing society as well as other high-level decision--making in other areas usually makes use of proper real data (economic, demographic, etc.) and agreed upon indicators (e.g. Gross National Product) that allow one to better understand what is to be regulated, to reason about the fundamental processes inherent to the area under consideration, to define the goals to be achieved, and to evaluate progress towards these goals. Availability of proper data and indicators calculated from them allow one to have feedback, to predict (and later on to evaluate) the impact of particular decisions, to measure the effectiveness of adopted measures, to improve our understanding of causes and consequences, etc. Unfortunately, cybersecurity is still a rather new area to be governed, and as of now there is no thought-out, generally accepted framework to systematically collect and process reliable (objective) data nor to assess them with the help of proper indicators to obtain deeper insight and to infer useful conclusions[1]. Clearly this has to be improved in order to decrease uncertainty about how much the decisions to be made reflect reality.

The need for proper fundamentals for high-level decision-making in cybersecurity and privacy protection in a form of reliable data has already been recognized by the Council of European Professional Informatics Societies (CEPIS) in its 2014 "Statement on Supporting High-level Decision Making on Cyber Security and Privacy Protection with Reliable Data"[2]. Illustrative examples given there were aimed mostly at privacy protection. Here we continue to apply and explore the idea within the cybersecurity area.

What Data For Cybersecurity?

There are several facets of this fundamental question. The decision on what data are needed to properly govern cybersecurity is closely related to the chosen preferred approach to tackling the problem.

[1] Instead, various (usually ad-hoc) surveys are used, replacing the objective data by an aggregate of a sample of subjective opinions.

[2] Statement on supporting high-level decision making on cyber security and privacy protection with reliable data, LSI SIN (14)01, CEPIS 2014 [online] http://www.cepis.org/media/Statement_Supporting_high-level_decision_making_with_reliable_data_Final1.pdf

For example, for the DAR approach (detect – attribute – retaliate) quite different data are needed than for an approach aimed to prevent incidents and/or to minimize their impact. While for the former case, mostly technical data (to enable early detection of an attack and its attribution) are needed, the latter one requires data and respective indicators that allow to reason in advance about likely targets, possible weak spots, attack vectors, strength of defences, etc.

Another facet differentiates between the need for long-term data on the characteristics of the cybersecurity “playground” (i.e. of the “know yourself”“type) and the need for short-term data on the actual state of defensive measures, observed events, etc.

Yet another facet exists between the data that are already collected (possibly for a different purpose but that could be used for a cybersecurity related scenario as well), thus instantly available and “for free”, and data whose collection needs to be properly organized possibly in a complex way, which takes time and might be costly.

This paper lacks the ambitions to provide an authoritative proposal for what data (and associated indicators) need to have solid fundamentals for realistic high-level decisions for the cybersecurity area. Instead, its aim is to provoke further discussion, hopefully converging to some generally accepted selection.

For practical reasons we suggest to start with “know yourself“ type of data, especially those whose collection does not require too much additional resources, i.e. data that can be obtained through the usual framework of statistical data collection or planned mandatory reporting of security breaches.

As an example consider the following questions – having data that make it possible to answer these questions provides for deeper insight into the respective parts of the cybersecurity “playground“ and allows for better tailoring of measures.

? QUESTION NR 1

What is the prevailing character of ICT (Information and communication technologies) systems used in the area under consideration (general, sectoral, …) – do they form a monoculture or is there enough diversity there? Are there observable trends towards the change?

Though a monoculture has clear economic advantages, it also causes much wider impact of even a single technical security vulnerability and such fact has to be seriously considered.

? QUESTION NR 2

What sectors are known to be attractive to what popular threats (e.g. identity theft, blackmail, hacktivism, espionage, etc.)?

Clearly systems operated within such sectors are more likely to be attacked, thus measures under consideration could be better tailored.

? QUESTION NR 3

What sectors under-invested in ICT and/or security in comparison to others?

Underinvestment in ICT and/or security increases the probability of successful attacks against the systems operated within such sectors\ combine that with the answer to the previous question (above) to get a more realistic picture on the potential targets of attacks.

? QUESTION NR 4

How many security experts are needed for subjects within a sector under consideration? What kind of expertise is needed or sought the most? How well does our educational system reflect such needs?

Clearly, the lack of proper expertise may hamper even a well-intended effort. Moreover, in this case there is a strong requirement to decide on proper measures well in advance.

? QUESTION NR 5

Where (in what sectors) are large amounts of attractive (personal or other sensitive) data aggregated in one place (organization)?

Clearly such characteristics increase the likelihood of intentional attacks aimed at such systems, but also possible impact of errors and unintentional mistakes made by users, administrators, and even suppliers of such systems.

The answers to the questions above allow to pinpoint where cybersecurity incidents are more likely to occur. On the other hand, other questions may be focused on the real state of security and allow to pinpoint where a more direct involvement might be urgently needed – for example:

? QUESTION NR 6

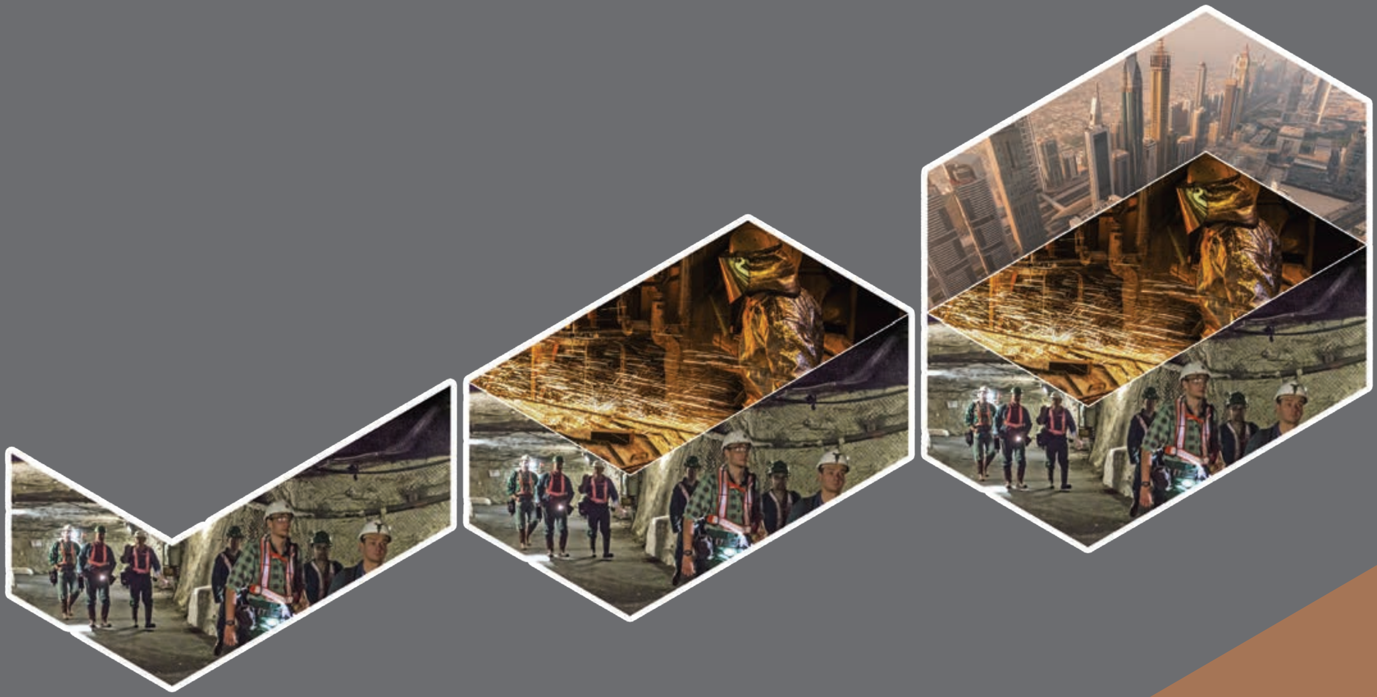
In what sectors are there systems that were recently used for attacking other systems abroad (based on complaints received)? What were the most frequent causes of security incidents reported?

And this is just the beginning.

The collection and evaluation of selected data over a time shows the effects (if any) of decisions made, measures adopted, the effectiveness of formal bodies tasked with specific roles and activities in ensuring cybersecurity, etc. Yet another option is that proper data collected over a longer time interval may reveal interesting trends and provide a basis for reasoned predictions for cybersecurity.

Summing it all together, there is a need for discussion and research on what data are to be collected and what indicators based on them help to cleverly tackle cybersecurity problems. ■

Layers of possibilities



KGHM
POLSKA MIEDŹ

Thanks to the knowledge and experience of our employees we extract and process the earth's precious resources, enabling development of the modern world.

ANALYSIS

THE REALITY OF CYBERWAR - CURRENT CONCEPTS AND FUTURE TRENDS

PROF. JARNO LIMNÉLL

The writer is the Professor of Cybersecurity in Finnish Aalto University. He also works as the Vice President of Cybersecurity in Insta Group plc. He has been working with security issues more than 20 years. Prof. Limnéll holds a Doctor of Military Science degree in Strategy from the National Defense University in Finland; a Master of Social Science degree from Helsinki University; and an Officer´s degree from the National Defense University.

Nowadays you can read news about "cyberwar" almost daily. Denial of Service attacks take down Internet websites, government ministries' information systems are breached and cyberespionage can reach even smartphones. News headlines and commentators' statements get a lot of attention when all different types of activities in the cyber domain are labelled cyberwar. This "cyberwar hype" needlessly excites the cyber arms race that is already underway, and unnecessarily creates an atmosphere of fear in societies. Not all events in cyberspace should be considered warfare. On the other hand, ever more powerful and skilled use of the digital domain and the extensive dependence of societies on functionality of cyber, force us to take note of this dimension of warfare. "Cyber", thought of as all actions in which the world of bits created by people has an effect, also affects all other dimensions of warfare.

Worldwide, we are just starting to build an understanding of what constitutes cyberwar and what does not. Still, we are not sure whether the concept of cyberwar should even be used. Some experts compare cyberwar to definitions akin to the war against drugs and poverty, and some declare that there will be cyberwar.[1] Disagreements over the concept show that we are only now developing an understanding of how the relationship between the events in the digital domain and warfare should be conceptualized.[2] There exist no precedents and so far it has been pretty *ad hoc* figuring out what's an annoyance and what's an attack.

[1] | E.g. Stiennon R., There will be Cyberwar, IT-Harvest Press, Birmingham 2015.

[2] | See e.g. Limnéll J., Rid T., Is Cyberwar Real? Gauging the Threats, "Foreign Affairs", March/April 2014.

In the physical world the issue is unambiguous. If a foreign nation's tanks operate in your territory, a war has likely already broken out. In the cyber domain the situation is different. Online espionage or Denial of Service attacks that do not cause serious physical damage are not cyberwarfare. And even if a hacktivist group targeted a massive attack at a nation's or country's critical infrastructure, it would not be a military attack but criminal activity. On the other hand, it is realistic to assume that serious information breaches or cyberespionage incidents will escalate and can possibly lead to the use of physical force between countries. In the existing situation, there are many open strategic questions related to the cyber dimension in warfare. Solutions and even some kind of shared international understanding of them are being sought. At the same time, the question of actors becomes more challenging. Although armed conflicts between non-governmental groups have also been referred to as war, at least one party is usually a country.

The current trend in cyber appears to be that if a country wants to use "more powerful methods in cyber" against its enemy, it can outsource the use of skills to non-governmental actors like activist groups that support the government.[3] In other words, the country itself can build usable cyberattack capabilities, but the actual operators are non-governmental actors and therefore provide plausible deniability. In this case, questions of responsibility and law are left unclear from the standpoint of defining war.

War Takes On Added Dimensions

In many countries, the cyber domain is now seen as the fifth dimension of warfare. It is considered comparable to land, sea, air, and space. Among others, the United States and Russia have established separate cyber commands and units in the military that are leading the development of military cyber capabilities and doctrines. The digital domain can in fact be seen as an operational dimension alongside previous dimensions, not replacing the use of physical force but creating a new operating environment that can be used for military purposes. The cyber domain offers a new option in the "toolkit for exerting power". Exerting power can include special operations that enable achieving goals similar to those achieved by using physical force.

> “ The cyber domain offers a new option in the toolkit for exerting power.

One reason for active development of offensive cyber capabilities is cost-effectiveness. A cyberattack is often cheaper, and in the minds of political decision makers a more cost-effective and deniable option for exerting power than the use of physical force. Cyberattack methods are also generally considered a "bloodless" way to exert power. The risk of troop losses decreases significantly when soldiers do not physically attack a target.

The digital domain is taken into consideration in military operations as its own operational dimension. Those responsible for exerting cyber power are included at the table when operations are being planned. For example, in a broad-ranging attack prepping the battlefield can now be done with "digital artillery" instead of physical artillery or aerial bombardment.[4] In the preliminary phase, cyberattacks can be used to disable a target's control systems, situational awareness, communication networks, or air-defence radar systems. In other words, exerting force in the world of bits can be used to create more favourable conditions for the use of physical force. Pure cyberwar, in which war is conducted only digitally is unlikely to ever occur.[5] Still, every war in the future will include a cyber-component. Cyberattacks can be used as an instrument to exert political and economic power, and in a serious crisis, as a way to exert force alongside traditional military methods. The use of traditional physical force will retain its place, but the cyber

[3] | Strasser M., Why Ukraine Hasn´t Sparked a Big Cyberwar, So Far, "Newsweek", March 18, 2014.

[4] | See as an example Israel´s possible plans to attack Iran. Mele S., Israeli attack against Iran will start with an unprecedented cyber-attack, [online] http://stefanomele.it/news/dettaglio.asp?id=320 (access 23.07.2015)

[5] | Can there be a "real" war that only takes place in or via cyberspace, without troop movements, conventional weapons etc.? See e.g. Ottis R., Cyber Warfare, [in] Cyber Security: Analytics, technology and Automation, ed. Lehto M., Neittaanmäki P., Springer, Switzerland 2015.

dimension makes warfare more multidimensional, complex, and challenging. It has to be remembered that the field of military cyber operations and cyberwarfare is still rapidly developing and therefore has not yet settled within the framework of more mature warfighting disciplines and technologies.

Another option is to recognize that at least in technically-developed countries the cyber domain permeates all levels and dimensions of warfare. It is difficult to imagine any land, sea, air, or space operations carried out without a digital component. The cyber dimension is not revolutionizing warfare, a level to which some experts have raised the importance of cyber.[6] It is simply normal evolution, in which warfare follows overall social development. War always embodies the special characteristics and technological development of societies. Today, societies are very dependent on the functionality of the digital domain, and are therefore vulnerable. If bits do not work, many things are left undone. The rise in importance of the world of bits in military operations may lead to changes in the balance of power. Skills are central to creating cyber capabilities. A country or non-governmental actor with fewer resources but the right skills can obtain capabilities and technological solutions that even superpowers do not have. Resources are needed, but their cost is in a different class than in the physical world. At its best, for a small and technologically sophisticated nation the cyber dimension is a cost-effective way to bolster its defensive capability.

A small nation may also have significant strengths compared to a large nation. The smaller one is often more agile, and cooperation between the public and private sectors is easier to organize.[7] This makes it easier to build trust, since operations are handled in a small circle and responsibilities are easily defined. A good example is Israel, which has for a long time invested in development of the right skills and their utilization, developing its military cyber capability through universal conscription. The technologically advanced State of Israel can be considered one of the world's most capable cyber nations.

The increasing significance of the cyber dimension has led many countries to focus on defending against attacks on critical infrastructure. Cyberattacks can cause serious disruptions and even destroy parts of infrastructure. For example, disrupting or disabling a country's financial system would have serious effects on its ability to function. Such an attack could cause stagnation of society or disruption of its functioning, weaken the national economy, hinder its ability to compete, and cause a decline in the quality of life. It is therefore important to protect critical infrastructure from both physical force and cyberattacks. The use of cyber force is primarily not directed at actual military targets. The most effective way to affect the enemy's society is to strike at critical infrastructure, i.e. civilian targets. Because the majority of critical infrastructure is owned and operated by the private sector, development has led to closer cooperation between the public and private sectors. For example, new forms of collaboration have been created. New legal responsibilities have also been established for the private sector.

Three Types of Cyber Capabilities

Even if, as a military capability, cyberwarfare is still finding its place among the other and often more mature disciplines, military cyber capability is made up of three capabilities: defence (protection), intelligence, and offense (ability to exert power). The goal of defence is to protect networks, systems, and technological components and to develop sufficient ability to recover from cyberattacks. The goal of cyber intelligence is to develop situational awareness and gather information required for protection and ability to exert power. A societal discussion about the need for offensive capability is ongoing in many countries. The discussion has occasionally been sidetracked. The development of the ability to exert power is considered the same thing as the use of cyber weapons. This is not the case. A country needs offensive skills for three reasons. First, if it wants to be a credible actor

[6] | "The future is moulded by the past. The best promise for the future lies in understanding, and applying, the lessons of the past. For that reason [...] more light may come from tracing the whole course of the revolution in warfare than by dealing merely with the appearances of the moment." G.H. Liddell Hart, The Revolution in Warfare, Faber and Faber LTD, London, 1946, p.76.

[7] | Limnéll J., Tabansky L., Governments need to protect industry from cyber-espionage – and some do, "SC Magazine", April 20, 2015.

in both security and defence politics and on today's battlefields, it must have a strong ability to operate in the cyber environment, including offensive capability. Second, offensive capability increases deterrence. Possessing and demonstrating strong capability prevent the use of cyber weapons against a country. Deterrence is everything. A credible deterrent raises the threshold for an enemy to launch an attack. Still, the bar is not high enough unless the nation also has offensive capabilities. Possessing capabilities is not, however, the same as using them. Third, both development of offensive strategy and building the ability to exert power are important in creating a strong and credible defence.[8] A country will not succeed by focusing only on defence. There must be an understanding of how an attacker operates and exercises to simulate attacks. This enables discovery of weak spots in the defences so they can be addressed. Effective and credible cyberdefence cannot be built without offensive capabilities.

Serious uncertainty currently reigns in the world concerning military cyber capabilities. Countries are not aware of each other's cyber capabilities. In the physical world, it is relatively easy to estimate how many tanks or fighter planes each actor has and how they plan to use them. Countries also reveal their arsenals in military parades and demonstrate their operational prowess in military exercises. This transparency exists because a deterrent only works if others are aware of it. In the world of bits, demonstrating capability and creating a deterrent are significantly more difficult. Cyberattacks usually do not leave behind physical evidence that could be used to determine where the attack was launched and who the enemy is. Even if an attack is known to have been launched from a certain location, we cannot be sure whether it was perpetrated by a government or by an activist group. Still, if perpetrators of cyberattacks are not caught, they also get no glory and are not able to demonstrate their capability. Recently, the developing trend has in fact been for various actors to openly take responsibility for cyberattacks that have been exposed.[9]

> “ Serious uncertainty currently reigns in the world concerning military cyber capabilities.

Countries will probably reveal their cyber capabilities more openly in the near future.[10] This can be done by organizing exercises and simulations that outsiders can attend and watch. The effects of cyberattacks done in laboratory conditions will be publicly reported. Presumably this will not, however, be sufficient to create a credible deterrent. Countries "must" demonstrate their capabilities in real situations and against real targets. This means cyberattacks against terrorist groups, hacktivist groups, industrial facilities, or even other countries. After a strike, the actor will take responsibility for it in order to make the cyber deterrent as great as possible. The logic is frightening but probable. Open demonstrations of cyber capabilities will no doubt lead to an escalation in the cyber arms race. The problem with exerting cyber power is increased by difficulty in differentiating it from the reigning philosophy of active defence. Passive defence is based on making targets as much of a "fortress" as possible. Today, however, there is increasing discussion of active defence, in which defence relies on active measures. This emphasises operations aimed at identifying and deceiving the aggressor. Active defence is also thought of as penetration of an attacker's networks and systems. The line between the principles of active defence and exertion of power is often debatable, since corporations have begun to apply the teachings of active defence.

It will be interesting to see how countries build their military cyber capabilities in practice. Probably only larger nations will be able to invest in building their ability to exert power independently. One option is to purchase the ability to exert power from weapons manufacturers. As with tanks, fighter planes, and submarines, the world's largest weapons manufacturers have been selling various cyber capabilities for years. This raises the question of reliability. How much can a co

[8] | Lewis J.A., The role of offensive cyber operations in Nato´s collective defence, Nato CCDCOE Publication, Tallinn Paper No.8, 2015.

[9] | E.g. DeYoung K, Nakashima E, U.S. hacks Web sites of al-Qaeda affiliate in Yemen, [online] https://www.washingtonpost.com/world/national-security/us-hacks-web-sites-of--al-qaeda-affiliate-in-yemen/2012/05/23/gJQAGnOxlU_story.html (access: 23.7.2015)

[10] | Limnéll J., Offensive Cyber Capabilities are Needed because of Deterrence, [in] The Fog of Cyber Defence, ed. Rantapelkonen J., Salminen M., National Defence University, Series 2, Article Collection N:o 10, Helsinki 2013.

untry's military rely on solutions produced by another country's weapons manufacturers? Production of cyber capabilities is nevertheless a rapidly growing industry.

The Cyber Arms Race

It can be estimated that today more than 100 of the world's militaries have some sort of organization in place for cyberwarfare and over 40 countries worldwide have published their National Cyber Strategy. Cyberthreats are also prioritized in many countries´ national threat assessments.[11] For example the latest worldwide threat assessment of the US Intelligence Community states that cyberthreats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact,[12] and Security Strategy of the Czech Republic emphasises how cyberattacks can cause particular failures of communication, energy, and transport networks, transport processes, and industrial and financial systems, resulting in considerable material damage.[13] In short, the danger of a disruptive and even destructive cyberattack is estimated to be growing and the escalating cyber arms race is currently underway.

> “We can say that a skilled person is the cyber domain's actual weapon.

The greatest competition is for skilled individuals, since expertise is the core of building cyber capabilities.[14] In cyber, talented and skilled individuals can achieve significant things on their own. The emphasis specifically on skills and asymmetry has led military and intelligence organizations, companies, as well as criminal groups to compete for who can hire the “lords” of the cyber domain. In a way, we can say that a skilled person is the cyber domain's actual weapon. Still, in a military sense it should be remembered that talented individuals alone are not enough. A successful cyber operation requires precise selection of a target, intelligence gathering, tailored development of malware, as well as measures used to deliver the malware to its target, which is done through both the world of bits and the physical world. If the target is for example an intranet not linked to the Internet, methods for delivery of malware to the target environment must be considered. Larger cyberattacks always require various skills for the demanding task of integrating the physical world and digital domain.

Does War Have To Be Violent?

Professor Thomas Rid is one of the best-known researchers of cyberwarfare. Rid does not recognize cyberwarfare now or in the future.[15] He bases his argument on the three criteria for warfare defined by history's most famous military philosopher, Carl von Clausewitz. First, war must by nature be violent. Second, the nature of war is instrumental, i.e. the goal is to make the enemy defenceless. Third, as Clausewitz's best-known thesis states, warfare is always political in nature and the purpose of war must be understood in a political framework. Rid's views are worthy of note when considering war in the cyber world.

The cyber domain must be seen as a dimension that can be exploited in war, either for independent operations or as part of a broader operation. Cyberwarfare is always part of a broader strategy of war. No nation or non-governmental actor wants to use its cyber capability just because it exists. An operation always has a purpose, i.e. there is always a reason for using the ability to exert power. According to Clausewitz, war is always an effort to achieve political goals. The cyber world offers an additional way to exert power. It is of course possible for political goals to be achieved by exploiting only the cyber dimension, in which case physical warfare is not even necessary. The use of cyber capabilities, therefore, does not yet start an actual war. A cyberattack alone does not necessarily lead to a declaration of war. “Cyberwar” is war in the sense of all wars. Still, the cyber dimension is used more easily

[12] Worldwide Threat Assessment of the US Intelligence Community, Feb 26 2015, 1. [online] http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (access: 11.7.2015)

[13] Security Strategy of the Czech Republic 2015, 13. [online] http://www.army.cz/images/id_8001_9000/8503/15_02_Security_Strategy_2015.pdf (access: 11.7.2015)

[14] E.g. Russian Defence Minister Sergey Shoigu has said the ministry had started a “big headhunt” to hire cyber personnel. In the United States the US Cyber Command has just half the staff it needs.

[15] Rid T., Cyber War Will Not Take Place, Oxford University Press, United Kingdom 2013.

than physical force even before an actual declared state of war. Various activities in the cyber domain can finally expand into actual warfare, which combines the use of physical force and power in the digital domain. Cyber actions must, in fact, be understood as part of strategy in an actual war.

The question of the violent nature of war is a difficult one in cyber. To exert power against an enemy through the digital domain, targets selected are primarily civilian, for example electricity and water distribution systems. How serious must an attack be in order for its target to legally declare a traditional war? How many civilian casualties lead to a declaration of war? Must someone die in an attack in order to make it grounds for a declaration of war, or is serious and long-term disruption of society's functioning sufficient? Compared to the physical world, the cyber domain has its own defining principles. Still, cyber operations must be seen as part of striving for political goals through warfare, but possibly without violent actions. The increasing activeness of countries in the digital domain has led to a blurring of the concepts of war and peace. If we believe that the opposite of war is peace, we do not even now live in an era of complete peace.[16] But we are still not in a state of cyberwar, either. Active exploitation of the digital world has blurred the concepts of war and peace, which are part of developing a definition of war. We currently live in a grey area between war and peace. An unambiguous definition of war is no doubt impossible because of the political nature of the concept itself.

In considering war in the cyber domain, we must examine Clausewitz's philosophy of war from a different viewpoint. For example, Clausewitz believed that achieving an advantage in warfare is based on defence and that offense requires significantly greater resources than building a defence.[17] In the cyber world the situation is different. Through the cyber dimension it is also possible to affect targets that cannot be accessed using physical force. History has shown that when new weapons of war are developed, they are also used. This will happen with cyber weapons as well. Today though, the world is so networked that the fear of unexpected side effects and multiplicative effects of a cyberattack restrains the use of such capabilities. Despite threats they may make, countries understand that they are networked and tied to cooperation with other actors. Exerting cyber power can strike painfully at one's own nest. Because bits know no bounds, there is a risk of friendly fire. It should also be ensured that decision-making is handled at a sufficiently high level before authorization to exert power through the cyber world is given. When the cyber domain is linked to all operations and war is aimed at achieving political goals, the constantly occurring conscious and unconscious exertion of information power must be seen as one form of warfare. It is a question of strategic communication.

Psychological warfare now plays a more important part in warfare and the art of war. Strategic communication is aimed at longer-term, more comprehensive influence, for example on a foreign government's decision-makers and the nation's citizens. An illustration is how Russia, in its own cyber strategy, uses the term "information environment" rather than "cyber domain," even though the strategy addresses today's concept of cyberspace. Conscious strategic communication using various information channels will increase in the future. We live in the midst of this phenomenon.

Rules Of The Game In Cyber

At the moment the cyber domain can be called the Wild West, where different actors do what they want without international controls or norms.[18] There are no rules of the game. We are at a critical juncture. We are developing cyber capabilities faster than policies and doctrines to control them. The Tallinn Manual on the International Law Applicable to Cyber Warfare sponsored by NATO's Co-operative Cyber Defence Centre of Excellence was an encouraging step forward in the pursuit of international norms and

[16] For example hybrid warfare can be seen as a more intelligent or efficient way to wage war because it seeks to achieve political goals without an extensive use of armed forces and violence. Using a range of tools such as cyberattacks, economic retaliatory measures, information operations, and limited physical attacks that generate uncertainty in the general population may be enough to achieve political goals.

[17] von Clausewitz C., On War, Indexed Edition, Princeton University Press, United Kingdom 1976.

[18] E.g. Kuchler H., Cyber world like "Wild West", say Obama, "Financial Times", February 13, 2015.

laws regulating the cyber domain.[19] But implementing and enforcing the norms the manual promotes has been poor. The world needs a fluid and frank dialogue among states, the private sector, and civil society in order to guarantee the security of cyberspace. There seems to be a desire for new normative and institutional orders in cyberspace, but what they might be, how they will be established, and how broadly they will be accepted are open questions. When considering cyberwarfare we should also take into consideration cyber peace and furthering it. The situation is most challenging with regard to espionage, an ancient phenomenon that has now moved online. Countries do not seem to have the will or the methods to contain it. Still, they have shared interests, for example prevention of cybercrime and extension of the rules of war to cyber. An international norm in the digital domain should be found. The situation is reminiscent of nuclear weapons after WWII. The international community first felt it was faced with an almost impossible challenge in considering laws and agreements to regulate nuclear weapons. But gradually, international rules of the game and methods for monitoring them were found.

> “ We are developing cyber capabilities faster than policies and doctrines to control them.

The power of the rules that countries agree to is that they gradually change the parties' behaviour, or at least force a country in breach of the rules to justify its actions under the scrutiny of the international community. The rules of the game are made up of agreements (words) and practices (actions). The ethical effect of the cyber dimension and its meaning for war in the future should also be considered. Traditionally civilians were considered out-of-bounds, which may be problematic when cyber capabilities are used to attack civilian infrastructure. Where should we start? Would it be better to negotiate an international treaty or to broaden existing agreements to cover the cyber world? The first option would probably be hard to achieve. Countries conceptualize the cyber domain in many different ways, and their interests are so multifaceted that finding a shared starting point is difficult. The latter option, for example including cyber issues in regulations on international trade and law enforcement, seems more promising. Some kind of a starting point for establishing rules of the game would already exist. Technology standards defined together would set out what tools of the game could be used. One option for creating international regulations would be to try to achieve shared rules of the game between two powerful nations. If shared rules could be established between the United States and China, they could serve as an example for the rest of the world and as a starting point for the creation of broader regulations. This is probably an easier way to approach the issue than by bringing all the countries of the world to the table. ■

[19] | Tallinn Manual on the International Law Applicable to Cyber Warfare, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, United States 2013.

FireEye®
SECURITY REIMAGINED

ONE **UNITED** DEFENSE AGAINST CYBER ATTACKERS

Today's cyber attacks are targeted, sophisticated and focused on acquiring your most sensitive information. They also go undetected by traditional security technology. Organizations need to reimagine security and adopt a Continuous Threat Protection model. This means having the ability to detect threats in real-time and reduce time to respond, thereby preventing or minimizing business impact. The FireEye Platform provides a multi-faceted approach to security – detect, prevent, analyze, respond.

DETECT

Signature-less and multi-flow virtual machine based approach that leverages superior threat intelligence

PREVENT

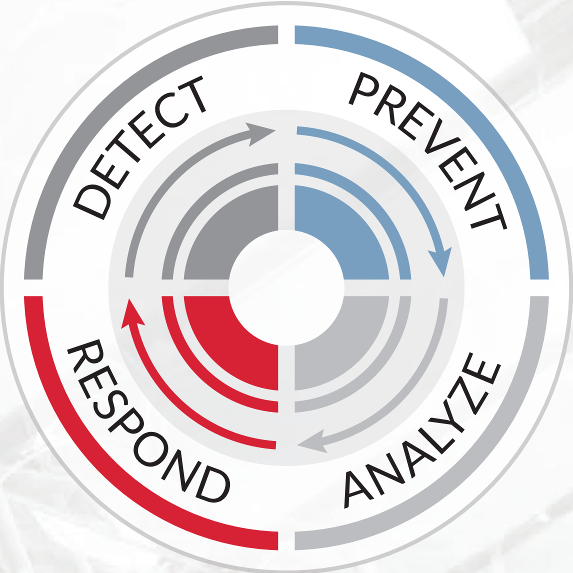
Multi-vector inline known and unknown threat prevention

ANALYZE

Containment, forensics investigation and kill chain reconstruction

RESPOND

Remediation support and threat intelligence to recover and improve risk posture



www.FireEye.com

ANALYSIS

CYBERDEFENCE COOPERATION BETWEEN NATO AND THE EU

BART SMEDTS[1]

Research fellow at the Centre for Security and Defence Studies (CSDS) of the Royal Higher Institute for Defence (RHID) since 2008. Graduated as Master in Aeronautical Science from the Royal Military Academy in 1989, he was appointed to air defence operations where he obtained all operational ranks. After a short graduation program in biotechnology in 1997, he obtained a Master in Science (chemistry) and joined the Royal Military Academy as professor assistant mathematics and chemistry. Forensic analysis of explosives and war agents the start-up of the Federal Orientation Laboratory against CBRN-threats in Peutie. His fields of interest ranges from proliferation issues, over critical infrastructure, cyberdefence and emergency planning.

Introduction

At the outcome of the Wales Summit, in September 2014, the importance of cyberdefence was underscored as follows[2]:

"the Alliance (...) recalls that the fundamental cyberdefence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks. Our policy also recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. Cyberattacks can reach a threshold that threatens national and Euro--Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyberdefence is part of NATO's core task of collective defence."

The obvious consequence of this statement is that cyberdefence is part of the collective defence effort and that its strength will fail at its weakest link. Therefore, national capabilities play a crucial role in the establishment of that collective cyberdefence effort and, due to the dynamic morphology of the threat in cyberspace and the entangled public as well as private interests, the Alliance's structure as well as the national capabilities in this domain have to be able to adapt accordingly. In this paper, the dynamic of this process will be shown from the very start of cyberdefence activities. Next, the legal basis and the broader picture of cyberdefence will be highlighted. Finally, synergies with the EU will hint to recommendations for improved cooperation.

History And Structure

The Distributed Denial-of-Service (DDoS) attacks during the NATO Balkan operations were only the onset of increased activity in the fifth domain. As a result, a number of cyberdefence tasks were developed and attributed to specific agencies within the NATO structure. The allocation of responsibilities has increased, along with the activities of the Alliance: it was for example decided during the Prague Summit of 2002 to launch the technical NATO Cyber Defence Programme involving a Computer Incident Response Capability (NCIRC)[3]. In April-May 2007, Estonia was harassed by DDoS-type cyberattacks: the impact on Estonian society was so deep that it was proposed to set up a centre of expertise (the Cooperative Cyber Defence Centre of Excellence-CCD CoE Tallinn) in order to promote cooperation and training between the NATO countries and to implement legislation for better resilience.

During the Lisbon Summit in 2010, it was decided that cyber was a vital part of the NATO Defence Planning Process (NDPP): the ensuing Policy and Action Plan focus on the defence of own networks, while the NDPP should guide the integration of cyberdefence in national networks[4]. Meanwhile, it became

[1] The views expressed in this paper are only those of the author and do not necessarily reflect the views or the policy of the Belgian Ministry of Defence or the Royal Higher Institute for Defence.

[2] Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales §72. Issued 05.09.2014. [online] http://www.nato.int/cps/en/natohq/official_texts_112964.htm (access 16.07.2015)

[3] MCM-064-02 dated July 2nd, 2002 (annex AC/322-D/0056).

[4] Herd G., Kriendler J. (ed.), Understanding NATO in the 21st Century. Alliance Strategies, Security and Global Governance, Routledge, London 2013, p.159.

clear that the military use of the cyber domain could extend to the civilian assets: the Stuxnet virus attack in Iran made clear that the targeting of high-value assets in a country that pays special attention to the security of its nuclear showpiece, would demonstrate that any western critical infrastructure is a potential target as well. Henceforth, it would be crucial for the future crises management to determine the possible consequences of any such type of attack and to find a legal basis for this rationale.

Legal Basis And The Bigger Picture

From the onset of the consultations with regard to the cyber domain, it was obvious that the resulting reaction in case of incident should be defined, more specifically it should be clear whether an incident falls under Art. 4 of the Washington Treaty which states that[5]:
"The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened".
or rather under Art. 5 which states that:
"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all ..."

One could argue about "compromised operability" if, in the process of determining that an attack is taking place on a NATO country, "consultation" is required. Obvious forms of aggression against critical infrastructure and information infrastructure tolerate no waste of time. However, it is not an easy task to determine whether a cyberattack falls under the conditions detailed in Art. 4 or Art. 5 of the Washington Treaty. In the Estonian case, for example, evidence could not trace without reasonable doubt the origin of the attacks. Already in 2008, before the NATO Bucharest Summit, the Secretary General Jaap de Hoop Scheffer specified that no aggressive attitude could be adopted in relation to cyberdefence and assumed that actions within this domain would fall within the terms of Art. 4. While it is now commonly accepted that international law also applies to the cyber domain, it is still required to shape definitions for terms such as "hostile act" and "hostile intent", which are actually not included in the Tallinn Manual. Consequently, the Rules of Engagement (ROEs) of the NATO response capacity should be clearly defined. Today, consultation is still required to recognise that an attack falls under the conditions of Art. 5 of the Washington Treaty as was the case after 9/11.

> "The Rules of Engagement (ROEs) of the NATO response capacity should be clearly defined.

One of the elements that required special attention since the first operational cyber steps were NATO's national capabilities. Therefore, the Cyber Defence Management Board has been negotiating with national representatives in order to set up a rapid intervention force. An essential part of the Alliance's response capacity is a network of national Cyber Emergency Response Teams (CERTs) which are responsible for the exchange of information and coordination essential to an effective and rapid response. Though almost 250 CERTs are operational worldwide, some NATO countries are still lagging behind in the development of national cyber policies that can be operationalised through their respective CERTs. Both the responsibilities and their organisational dependence are not standard in NATO countries and therefore their coordinating role is not either: whereas in seven nations (Austria, Czech Republic, Germany, Estonia, Hungary, Latvia, and Turkey) Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) coordination are contained in separate bodies, it is linked in three others (Spain, France, and the Netherlands) or held by the same authority (Belgium and Italy)[6]. It should be added that national plans for the protection of critical information infrastructure in member states or an ad hoc response plan are not always in place[7].

[5] | The North Atlantic Treaty, NATO Public Diplomacy Division, Brussels.

[6] | Kaska K., Trinberg L., Regulating Cross-Border Dependencies Of Critical Information Infrastructure, NATO CCD COE Publication, Tallinn 2015, p.11. [online] https://ccdcoe.org/multimedia/regulating-cross-border-dependencies-critical-information-infrastructure.html (access 16.07.2015)

[7] | EU Cybersecurity Dashboard, A Path to a Secure European Cyberspace, BSA - The Software Alliance, 2015 [online] http://cybersecurity.bsa.org/ (access16.07.2015)

But restricting the fifth domain to cyber is missing the complete operational picture: NATO's cyberdefence does not stand on its own, but fits in the larger operational C4ISR[8] architecture essential to operations. The acronym has many derivate definitions specific to the means that are allocated, but the final goal remains the same in each case: "The provision of information and intelligence to commanders that enables decision superiority necessary to execute the Commander's Intent, along with the appropriate level of situational awareness, to the point of achieving the desired effect"[9].

The Alliance is the example of a military C4ISR architecture based on the experience of one of its largest constituents, the United States: the network-centric warfare (NCW) concept of the US was translated into the smaller-scale UK Network-Enabled Capability (NEC) and has extended beyond the sole military needs in those countries: it has not yet occurred to all other allied countries that, in order to meet operational requirements of interdependence, interoperability and integration, the strive for C4ISR interoperability is based on the same principles as the cyber requirements, being the implications of civil as well as military capabilities in order to complete the picture. It should therefore be concluded that the operational management of ICT and derived systems is no easy task in practice. First, NATO should be vigilant to maintain the operational capability of the Alliance, taking into account that cyber fits in a larger architecture supported by smaller national capabilities: it should not be split in a group of top players and less capable member states. Second, given the fundamental difference in approach of the Alliance as compared to the EU (and its member states), the former as a military alliance, the latter as economic commercial alliance. The motivation of the latter can consequently be far different with regard to operational security issues and extend beyond the sole military function: vulnerabilities outside the military capacity of Allies/ member states (e.g. critical energy infrastructure and its industrial control systems) can therefore have consequences for the Alliance.

Synergies Between NATO And The EU

Interoperability still is a critical issue for coordination between NATO and the EU. This applies not only to operational deployment (e.g. during emergency planning), but also in the field of cyberdefence: both NATO and the EU are sustained by the member state networks. Knowing that information networks are interconnected and interests of private and public sectors are entangled, cooperation between sectors and institutions are crucial to build up a robust information infrastructure. As stated, the C4ISR picture extends beyond the sole military domain and therefore NATO needs the EU: EU's support to the creation of a national network of CERTs was mentioned. The NATO-CERT that acts as a coordinating body during the operations of the Alliance, is embodied by the NCIRC: it will, however, lose operational power if not all countries participate in their effort to create a national CERT that has the means to field a cyberdefence policy which has been coordinated or has at least common ground with cyber policies of other Allies. Although such a responsibility should be left to the member states, it should be underscored that there can only be a "global" approach to create successful cyberdefence.

> "Interoperability still is a critical issue for coordination between NATO and the EU.

One possibility to test the present status of resilience consists in the organisation of exercises, both nationally and internationally. It is to be concluded that the US precedes both NATO and the EU in this field: in 2006 already, a major exercise was conducted (Cyber Storm I) between the US, Great Britain, Canada, Australia, and New Zealand to test existing procedures with regard to resistance and effectiveness during attacks. The 2008 version of the exercise (Cyber Storm II[10]), assumed that the enemy could penetrate any network and attack SCADA systems of critical infrastructure[11], amongst which Critical Energy Infrastructure (CEI).

[8] | Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition and Reconnaissance.

[9] | The Joint Air Power Competence Centre (JAPCC) Roadmap for Air C4ISR in NATO, version 1.0, November 2007. p.3.

[10] | Cyber Storm II, National Cyber Security Exercise: Final Report. Australian Government, Attorney-Generals Department, Security and Critical Infrastructure Division, August 2008.

[11] | Enhanced resilience against cyberattacks on SCADA systems is underscored in COM(2009) 273 final- Annex 1 to EU CBRN Action Plan (action C.9 of goal 2 : enhance the security of high risk CBRN materials and facilities-chemical).

The 2013 and 2014 NATO versions of cyber exercises demonstrated an increase in participation and complexity of scenarios, yet it is only the 2015 "Locked Shields" version of the exercise that included new attack vectors using Industrial Control Systems (ICS) and Supervisory Control And Data Acquisition (SCADA). Coordination of action for the protection of CEI would indeed improve the effectiveness of both organisations. Although energy constitutes one of the sectors supported by the European Programme for Critical Infrastructure Protection (EPCIP), the EU has a different definition of CEI terms than NATO[12]: the nature of criticality is often determined by the impact of the damage to infrastructure and other dependent site infrastructure, services and industry. Vulnerability is hereby reduced to the physical, human and IT aspects.

> Increased CIIP cooperation and training between the EU and NATO could improve existing synergy.

This approach needs to be reviewed with regard to dependencies between sectors and the potential to induce cascades of failure between sectors. It should therefore be underscored that the impact of damage in one sector (military or civilian) needs to be anticipated. Yet the cascade-inducing potential of an attack is equally important. As a result, the Alliance, unlike the EU[13], acknowledges the importance of both its own infrastructure and the infrastructure outside the territory, ensuring for example the energy supply to the Alliance (such as ports, transport routes, pipelines, terminals, and the interconnection between electricity grids). Different national approaches can be found inside the EU. However, the supranational approach can provide a better (overall) understanding of the problem to ensure synergy between EU and NATO efforts. The EU emphasises more the protection of national critical infrastructure (and the coordination of national approaches), a critical infrastructure being earmarked as a European Critical Infrastructure when its disruption or destruction would have a significant impact on at least two member states (Directive 2008/114/EC). Synchronising the EU and NATO would imply that NATO is able to focus more on the protection of external infrastructure (through projection and intervention capacity), whereas the EU would focus on ECI. Moreover, collaboration between the EU and NATO could improve resilience by diversification of tasks, inhibiting duplication or dilution of deployable resources. As an example, we could already pay attention to both the physical and cybernetic protection of alternative energy exploitation infrastructure and how to organise/synchronise this objective between the EU and NATO.

In view of these different approaches, increased CIIP cooperation and training between the EU and NATO could improve existing synergy. Cooperation between the European Union Agency for Network and Information Security (ENISA) and the CCD CoE, for example, could lead to successful informal results. The formal level is more difficult to reach since nations are very reluctant to release sensitive information, let alone to rely on the supranational level to synchronise it. Worse, it is at national level often not always clear whether a CERT authority would organisationally be better under the supervision of the military, a public service, an academic institution, a police department, or other private partners. It remains a political decision to decentralise resources, let alone denationalise their supervision to a supranational body/authority. In a purely military context, this is feasible with an integrated NATO command, but within the EU, with CI(I)P domains being dispersed over different directorates and services, it is still a problem for its civilian tier as well as for its military tier (with cyberdefence efforts dependent on member state cooperation). A consistent approach to definitions related to CI(I)P and its civil as well as military consequences would benefit the collaboration in both organisations.

[12] | Energy security: Co-operating to Enhance the Protection of Critical Energy Infrastructures (157 CDS 08 E rev 1), NATO Parliamentary Assembly, 2008 Annual Session. The report underscores that physical attack demands other response than politically motivated disruption of energy resources.

[13] | The existence of external connections is not denied, but the organization of defence is fostered in sectoral agreements.

Recommendations

A long-term vision and rationalisation on CIP/CIIP integration in a strategic plan or a concept is needed: in order to cope with the volatile and cross-domain threats, nations and international bodies have to establish the framework within which the policies will lead to tangible results capable of improving the resilience in the sectors that are most exposed to damage/cascading events as a result of a cyberattack. The search for synergies has demonstrated that a lot of work remains to be done in the field of distribution of tasks between the EU and NATO. Interoperability should therefore be further pursued, also with UN partners. The observation that ICT capacity is stretched between a military and a civilian tier should lead to enhanced cooperation in order to reach a holistic and integrated approach so as to integrate within a C4ISR architecture that benefits both the military and the civilian world. This objective reaffirms the need for cross-sector exchange in the form of combined training and exercise, mitigation, detection and early warning, response, recovery and exploitation of lessons learned. For example, special attention will be required in the future for the cooperation in the security of critical energy infrastructure. Military operations are dependent both on this infrastructure and supply chain preservation. The NATO Industry Cyber Partnership, launched in September 2014, is expected to improve this preservation as well as to contribute to the cooperation of military with private partners in mutual information sharing, in cyberdefence education, training and exercises. This could constitute an opportunity to have the EU join one more cooperation platform: the growing importance of private partners deserves even more attention in the future.

In a context of credit crunch and global, volatile threats produced in the fifth domain, a multi-departmental and multilateral effort will be the bottom line to reach a satisfying level of security. It will be difficult, however, to establish priorities. Reduced efforts in the field of tactical and strategic security in our own territories are a dangerous trend, as the loss of service in any field whatsoever will compromise the essential foundations of our society: an immediate impact on our daily lives cannot be excluded. Protecting national critical infrastructure vulnerabilities against asymmetric cyberthreats needs coordination: in a context of "rationalisation", the task of a supranational body may become even more important and burdensome in providing an organisational, legal and operational common ground. As a consequence, new equipment (including ICS/SCADA) from different origins should be submitted to internationally agreed certification standards in order to ensure interoperability and compatibility. We have already mentioned the urgent need to rationalise early warning systems and communications between the different NATO, EU and UN entities: military information networks and communications cannot be totally isolated from the complementary information grid constituted by C4ISR network elements and should therefore be resilient to cyberattacks. Expeditionary forces are more and more relying on network-enabled information exchange. Protection of CI(I) is crucial to the successful completion of the missions. Interoperability should consequently be a priority for EU, NATO or UN operations. A lot remains to be done in the field of interoperability, especially at the level of the UN.

An international body at EU level, coordinating the emerging threats and risks for the benefit of the member states should include the resilience on CI(I)P issues. The difference in policy between NATO and the EU should therefore be revised in order to enable coordinated action in case of disruption. Besides differences in policy, definitions should be standardised in view of compatibility, for example with regard to the rules of engagement to be applied in case of incident. Definitions, strategy and policy should for this reason consider consequences of CI(I)P cascade effect and consider the cross-sector impact of a cyberattack on CI.

> “ A long-term vision at national level is the cornerstone of the targeted ambitions.

A long-term vision at national level is the cornerstone of the targeted ambitions. This also applies to the EU:

as NATO's strategic concept is regularly subject to revision, the EU should also work towards a strategic vision that fits into a complementary framework of cooperation, with clear agreements on responsibilities, without duplication of duties and continuous engagement for optimal interoperability. Redefining the position of supranational institutions becomes therefore necessary. If the effort has been done to improve communication and collaboration between the EU and NATO, a lot remains to be done to streamline cyberdefence efforts.

Conclusion

Since the appearance of the cyberthreat, events have proved that it is real, permanent and asymmetric in nature. Both the conceptualisation of the threat and the organisation have improved since the demonstration of Stuxnet consequences and all of the subsequent events. Even the legal aspects of the use of force in the fifth domain have been studied, in theory at least. In practice, the development of events has illustrated that the concept is not that easy to apply and holds consequences for collateral damage that are not necessarily under control yet. Old concepts often need to be updated in the light of their implications due to the appearance of cyber applications. Sovereignty is one of them, as there is no such thing as a cyber territory and not a single nation nor department of that nation that are able to develop and field an operational cyberdefence that bolsters a C4ISR architecture on its own. The absence of state borders in cyberspace as well as the dependence on industrial control systems and smart grids in the near future highlight the threat of a cyberattack that could be launched from anywhere in the world without the certainty to be able to detect it, let alone identify the attacker, in due time. Therefore, early warning and consultation upon ongoing cyberattacks beyond the intensity that can be classified under the use of force will have to be fast and effective. The decision to classify under Article 4 or 5 of the Washington Treaty may be clear when such an attack is concomitant with traditional force deployment, it may be not that obvious at the onset of conflict to determine what a proportionate reaction could encompass, especially in the case of cascading effects and possible consequences in own civilian sectors, such as critical energy infrastructure.

Both at national and supranational level, adjustments should therefore be imposed on definitions, methods for early warning and cyber forensics, and distribution of responsibilities: the interpretation of the CI(I)P concept has a different meaning in different institutions, with consequences for the identification of national and transnational critical infrastructure, and the measures that would be provided for their protection.

Opportunities for synergies between the EU and NATO being examined, a defect appears to exist in the definitions, information exchange, capabilities and objectives between the two organisations but even more so with the UN. CIP and CIIP will remain on the agenda as disciplines that need improvement since failure could generate cascading effects on the military operational status of member states and Allies but evenly on the functioning of civil society.

The Wales Summit declaration describes future cooperation between NATO and the EU as follows: "We look forward to continued dialogue and cooperation between NATO and the EU. Our consultations have broadened to address issues of common concern, including security challenges like cyberdefence, the proliferation of weapons of mass destruction, counter-terrorism, and energy security. (...) We welcome the Secretary General's report on NATO-EU relations. We encourage him to continue to work closely with the EU High Representative and the leaders of other EU institutions across the broad spectrum of the NATO-EU strategic partnership and provide a report to the Council in time for the next Summit"[14].
The next Summit will be held in Warsaw: the cooperation and partnership between NATO and the EU extend beyond the usual operational improvement. It should include the proper delegation of cyberdefence responsibilities on the one hand and the protection of critical infrastructure prone to cyberattacks on the other hand. ■

[14] Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, §104 and 106, issued 05.09.2014 [online] http://www.nato.int/cps/en/natohq/official_texts_112964.htm (access 16.07.2015).

UP-COMING PROJECT

NATO ROAD TO CYBERSECURITY

The expert project creating recommendations on the most critical aspects and challenges of NATO's cybersecurity policy before the 2016 Summit in Warsaw!

- Cyber aspects of hybrid warfare
- Cyberattacks and Article V
- NATO cybercooperation with the EU
- Offensive cybercapabilities
- Cooperation with the private sector

Get involved!

THE KOSCIUSZKO INSTITUTE

OPINION

EUROPEAN CYBERSECURITY: TODAY'S DECISIONS ARE TOMORROW'S TERRAIN

J. PAUL NICHOLAS

Paul Nicholas leads Microsoft's Global Security Strategy and Diplomacy Team. He recently served as subject matter expert for the East West Institute's 2011 publications, including the first U.S. Russia taxonomy for cyber collaboration and a review of the applicability of The Hague and Geneva Conventions on cyberspace. In 2007, he helped to establish the Software Assurance Forum for Excellence in Code (SAFECode), a multi-company effort to advance industry best practices for software security and integrity. Prior to joining Microsoft, Paul spent over eight years in the U.S. Government, focusing on emerging threats to economic and national security. Paul earned a B.A. from Indiana University, an M.A. from Georgetown University, and is a Certified Information Systems Security Professional.

The cybersecurity policy decisions we make today will shape the cybersecurity terrain of tomorrow. Discussions related to cybersecurity have reached a near fever pitch over the past few years. As reliance on technology has grown, the pace of cyberattacks has become near relentless, with attacks increasing in intricacy, damage inflicted, and complexity of the motivating factors. As a result, bolstering cybersecurity has become a priority for boardrooms and government officials around the world.

Microsoft welcomes this new focus on cybersecurity and is committed to working with customers and partners across the public and private sectors to find and implement solutions that can help increase the stability and reliability of our products and services, but also of the online environment as a whole. We realize that ultimately people will not use technology that they do not trust, and that it is up to the technology industry to establish the fundamental levels of trust and security that are essential for new digital solutions to succeed and in turn enable growth and opportunity that they promise.

However, cyberspace is unique in that almost everything requires cooperation between the different stakeholders involved. The same is true for cybersecurity as governments have an important role to play in partnering with the private sector to not only secure their own systems, but those of their citizens and critical infrastructures. Moreover, cyberspace is also unique in that in almost all instances international cooperation elevates rather than compounds the challenges and threats faced, even if the task seems impossible at first glance. Unfortunately, the picture that Europe paints today in that regard is a patchwork of approaches, partnerships, and diverging levels of security. It is time to get it right.

> “ We realize that ultimately people will not use technology that they do not trust, and that it is up to the technology industry to establish the fundamental levels of trust and security.

The European Commission realized the need to act and adopted the European Union's Cybersecurity Strategy in February 2013. The Strategy is a set of non-legislative measures on a broad range of cybersecurity issues, underpinned by the Commission's overarching desire to establish a secure digital single market for Europe and to ensure the smooth functioning of the internal market. The Commission's concerns about the scale of the risk posed by cyberattacks emerged as a result of the ever-increasing digitalization of the economy and the acknowledgement of the fact that “there is currently no effective mechanics at the EU level for effective cooperation and collaboration for secure information sharing on cybersecurity incidents and risks among the Member States”. A crucial part of the strategy developed to address this challenge is the proposal for a Network and Information Security (NIS) Directive.

While the proposal has been making progress in the intricate inter-institutional discussions, the scope of the Directive remains the key challenge with policy makers struggling to balance and understand requirements for asset based infrastructure services (physical) versus information based services (virtual). Asset based infrastructures traditionally deliver services within a country and are governed through national regulations. In contrast, information based services are delivered across national boundaries and are governed by contracts and service level agreements that meet requirements set by asset based infrastructures, as well as public and private enterprise requirements. If the Directive does not strike the right balance, it will be very damaging to European security and innovation. Applying unique national cybersecurity requirements in EU Member States will not improve cybersecurity and unfortunately, will also impede innovation of service.

> “ The lack of public-private cooperation represents a critical gap in current levels of cybersecurity protection across Europe.

The latter point is critical. The directive should determine precise criteria and should not allow the Member States too great a leeway for their own regulatory formulations. From an industry perspective, creating products or services that must meet divergent, or worse, conflicting national requirements is unworkable and unnecessary. As Member States, the European Commission, and the European Parliament are in the process of finalizing the NIS Directive, they should ensure that the emerging legislation pursues a harmonized, risk-based, transparent, and technology-neutral approach.

We urge the Council and the European Parliament to ensure that the final compromise is respectful of these principles which have also been enshrined in the Digital Single Market (DSM) Strategy recently published by the European Commission.

Furthermore, the DSM Strategy also aims to build confidence in the digital sector. In that context, and as part of the DSM Strategy, the Commission is expected to launch a Public-Private Partnership on Research and Innovation in Cybersecurity later this year to foster the deployment of secure networks and services. This will also work towards greater interoperability and recognition of standards in Europe. Last but not least, the European Agenda for Security that was released on 28 April 2015 features cybercrime as a key priority. This agenda also puts a strong emphasis on public-private cooperation as a means to collect evidence and information, better react to cyberattacks, and enhance cyber capacity building action.

As highlighted earlier, the lack of public-private cooperation represents a critical gap in current levels of cybersecurity protection across Europe, and it is pivotal that the opportunities provided by the legislative proposals are grasped with both hands by Member States. A closer look at the situation on the ground reveals that whilst most critical infrastructure is owned and operated by the private sector, making public-private cooperation on cybersecurity is essential – only five Member State have established frameworks enabling it - Austria, Germany, Spain, UK and the Netherlands. An important improvement that could be achieved by the NIS Directive would be the creation of platforms for dialogue between the public and private sector on cyberthreat trends and developments and to promote EU-wide exchanges on industry and government cybersecurity best practices. The more communication and coordination is taking place between EU governments and the private sector, the more resilient Europe will be in the face of evolving cybersecurity threats. This effort will become even more important with the uptake of newer and more complex technologies, such as cloud computing and the Internet of Things. ■

POLICY REVIEW

CYBERSECURITY LEGISLATION IN THE CZECH REPUBLIC

TOMÁŠ REZEK

Tomáš Rezek graduated in International Trade and Commercial Communications at the University of Economics in Prague. He accomplished a stipend study on international trade and mathematical programming program at the University of Edinburgh. In 2015, he successfully defended his thesis on cyber terrorism at the Institute of international studies, Charles University. For several years, Tomáš worked with global consulting company as a consultant in the field of IT and currently works as a project manager at the information management department at a major Czech bank.

1. Introduction

It has been more than two years from the largest cyberattacks on Czech websites. The media paid a lot of attention to these attacks as the first wave targeted the main news portals in the Czech Republic. The second wave targeted financial institutions. Despite the media attention the attacks suddenly ended, as surprisingly as they had started. According to security experts, no serious damage was caused. Attackers used the the Distributed Denial-of-Service (DDoS) method method to disrupt the functionality of targeted websites, so people did notice that something is going on as they were not able to access their emails[1], but the media started to bring up famous cases from abroad and describe various catastrophic scenarios related to cybersecurity issues. It was probably thanks to these incidents that the public acknowledged that the responsibility for this domain is in the hands of the National Security Authority (NSA). The NSA was given the authority over cybersecurity in 2011. The Parliament passed the resolution on 19th September, 2011 and took the responsibility from the Ministry of Interior, where the police and other offices were attempting to address this area. It took four years to prepare and pass the necessary legislation to confirm the position of the NSA. By chance, the attacks occurred when the law on cybersecurity was discussed in the Parliament. As the NSA officials say with a smile, it was the best promotion for the law. The law on cybersecurity came into force in January 2015.

Four years have passed since the NSA got involved in the domain of cybersecurity. A tremendous progress has been made since then, there is no doubt about that. The NSA increased its international cooperation on cybersecurity by sending an expert to the NATO Centre of Excellence in Tallinn, and established a virtual cyber shooting range[2] in Brno together with the centre for cybersecurity. The question is, whether the actions taken during the last years made up for the delay the Czech Republic had in the field of cybersecurity when compared to other EU states.

2. Legislative Framework For Cybersecurity

The law on cybersecurity is the flagship of the NSA regarding the national approach towards security. It consists of several legislative documents – the law on cybersecurity (181/2014 Coll., from 23rd July, 2014), a governmental order changing the criteria for the identification of a critical infrastructure component (315/2014 Coll., from 8th December, 2014), a governmental notice on cybersecurity (316/2014 Coll., from 15th December, 2014), and a governmental notice on important information systems and identification criteria (317/2014 Coll., from 15th December, 2014).

2.1 The Law On Cybersecurity

The law on cybersecurity was drafted by the NSA in close cooperation with law experts from the Masaryk

[1] | The Czech Republic is one of the few countries in the world where Gmail and Google related services do not have a superior position on the market. A significant number of users use a local company Seznam for email address provision.

[2] | The shooting range was established with the Masaryk University in Brno and it was inspired by similar facilities in the USA or in Israel. It is practically an isolated network, where teams can simulate different attacks and defence tactics in isolated environment with the possibility to analyse the process afterwards.
CTK, Češi budou v Brně nacvičovat obranu proti kybernetickým útokům, 29th April 2015, [online] http://www.novinky.cz/internet-a-pc/bezpecnost/368321-cesi-budou-v-brne-nacvicovat-obranu-proti-kybernetickym-utokum.html, (access: 20.06.2015)

University. The draft was submitted for comments to a wider audience including different governmental bodies, bodies, Internet Service Providers (ISPs), NGOs, and private, NGOs, and private companies. The final document was afterwards submitted to the Parliament. The law itself is not very complex, as the purpose was clear – confirm the responsibility of the NSA towards the issue of cybersecurity and define basic terminology.

> “ The law on cybersecurity is the flagship of the NSA regarding the national approach towards security.

The law defines critical information infrastructure as a system or an item from the critical infrastructure in the field of communication and information systems with regards to cybersecurity. In other words, only systems, networks, or items directly related to critical infrastructure can be regarded as part of critical information infrastructure. Critical infrastructure is defined in the law on crisis management (240/2000 Coll., on crisis management) and selected according to given criteria. Critical infrastructure is organized in nine groups as defined in the governmental notice:

- Energy (Electricity, Gas, Oil products, Heating)
- Water management
- Agriculture
- Medical care
- Transport
- Communication and information systems
- Financial market and currency
- Emergency services
- Public services[3]

Within the communication and information systems group is the definition of a critical infrastructure item related to cybersecurity:

- An information system influencing the operation of a critical infrastructure component, with inappropriate replacement costs, or replacement period longer than 8 hours;
- A communication system influencing the operation of a critical infrastructure component, with inappropriate replacement costs, or replacement period longer than 8 hours;
- An information system managed by the public sector containing personal data on at least 300 000 persons;
- A communication system providing a connection of a critical infrastructure component with guaranteed data transfer capacity of at least 1 Gbit/s.[4]

The law also specifies the roles of the national and governmental Cyber Emergency Response Teams (CERTs). The governmental CERT is established within the NSA, whereas the role of the national CERT is outsourced to a private entity.

Important information systems and important networks are also defined by this law. Important information systems are the systems that are managed by the public sector and these systems do not qualify as critical information infrastructure, but their disruption would have an impact on public sector functions. Important networks provide a direct foreign connection into public communication networks or provide connectivity to critical information infrastructure. Important information systems and their detailed identification criteria are based on the notice issued jointly by the NSA and the Ministry of Interior.

The obligation to report incidents and security breaches is established in the law as well. It also defines roles, in which dedicated staff is obliged to communicate with the NSA and defines a cybersecurity event (an event which might cause a cybersecurity incident) and a cybersecurity incident (a violation of data security/integrity in information systems and networks). The responsible persons have to report security incidents immediately after detection to the national CERT (incidents in important information networks) or directly to the NSA – the governmental CERT (incidents in critical information infrastructure or important information systems).

In reaction to the gathered intelligence and reports from international partners or domestic CERTs, the NSA has the authority given by this law to issue warnings, reactive measures, and protective measures. Reactive and protective measures have to be imple-

[3] Zakonyprolidi.cz: Předpis č. 432/2010 Sb.Nařízení vlády o kritériích pro určení prvku kritické infrastruktury, (22nd December 2010), [online] https://www.zakonyprolidi.cz/cs/2010-432, (access: 21.06.2015)

[4] Ibid.

mented in critical information infrastructure, important information systems, or important networks. The NSA can declare the state of cyber danger. The state is declared for a maximum of seven days. It can be prolonged by the NSA, but the duration of the state cannot exceed thirty days. When the state of cyber danger is declared, reactive measures declared by the NSA have to be implemented by ISPs and in important information systems. The announced measures have to be implemented without delay.

To sum up, the law confirms the authority of the NSA over the cybersecurity domain, but at the same time it limits its authority only to a particular part of cyberspace. Critical information infrastructure has the most obligations given by this law. It is derived from the critical infrastructure. It is a logical step. However, the law inherits the problems related to the definition of critical infrastructure. For example, chemical plants are missing on the list. Therefore information systems operating chemical plants cannot be regarded as a part of Czech critical information infrastructure and they are not under the authority of the NSA.

2.2 Governmental Order 315/2014 Coll

The purpose of this order was to adjust the detailed criteria for the different critical infrastructure groups as defined by the governmental order on criteria to define a critical infrastructure component (432/2010 Coll.). The order changes the detailed parameters, not the nine groups listed above.

2.3 Governmental Notice 316/2015 Coll

This governmental notice was drafted by the NSA and it sets some cybersecurity standards applicable to entities specified above by the law. It also gives more detailed information on the communication patterns and defines basic terms used in the law. The notice defines the obligation for critical information systems managers to conduct a security audit at least once per year with a focus on cybersecurity. The management is also obliged to set up and use risk management methodology and to define its security policy with a focus on a list of defined topics (ranging from supplier management to secure usage of mobile devices). The obligation to ensure organizational security and to define security requirements for suppliers is applicable also to the management of important information systems. This applies also to the obligation related to information assets management, human resources security, operation and communication management, or to business continuity planning. There are special requirements singled out for the management of critical information infrastructure. Technical security standards cover mainly the level of encryption and the approved algorithms for the encryption of personal or sensitive information. It also mentions basic rules for password policies in affected entities as well as activity logging for audit purposes. It states that all users must have a unique identifier under which their actions in the system can be tracked, the passwords for such accounts have to be changed regularly, and they have to meet the minimal requirements mentioned in the notice. The notice also specifies which applications have to undergo penetration testing, and what documentation has to be available for the used applications or systems.

> “The law confirms the authority of the NSA over the cybersecurity domain, but at the same time it limits its authority only to a particular part of cyberspace.

Failure to comply with this notice is punishable by the law. The penalty is defined for a legal entity as 100 000 CZK and 50 000 CZK for a physical person. Regulatory authority in the respective field might also use this failure as an argument to start its own investigation.

The governmental notice gives more information on the incidents as it defines different types of incidents based on the cause of the incident or on the consequence of the incident. A standard form for incident reports is also part of the notice. The attachment to the notice defines official scales for measuring the confidentiality level, the integrity level, and the availability level of the information asset. The scales for risk and threat assessment are also part of this document.

2.4 Governmental Notice 317/2015 Coll

This notice defines the criteria necessary to identify important information systems. The identification is based on two main criteria – the impact and area of activity.

The impact of a security incident is defined from two perspectives. The first one is the impact on the provision of services by the state. The disruption of a system might disrupt the operation of a public authority or the provision of information to the public; or the management of a supervisor of critical information infrastructure or important information system; and the disruption would be longer than three days. The second perspective is more focused on the real consequences. The disruption of the system may jeopardize a critical infrastructure component; cause more than 10 casualties or seriously injure more than 100 people; cause damage estimated as greater than 5% of the budget of a given public authority; impact private life of more than 50 000 persons; or significantly jeopardize public interest.

The area of the activity criterion is basically defining which activities of the public sector in combination with the impact criterion lead to the identification of an important information system. In other words, an important information system can only be an information system operated by a public authority used for the listed activities with possible impact as defined by the governmental notice. In total, 92 systems have been identified as important information systems by this notice.

3. Conclusion

The legislative framework appears to be sufficient to commence more efficient governance of cybersecurity in the Czech Republic. Nevertheless, since it is based on the existing laws defining the critical infrastructure, the imperfections of this law are transposed into the legislation related to cyberspace. Amendment to critical infrastructure legislation is needed, or at least an update of related governmental notices. The selection process of critical infrastructure is crucial for its protection. It is possible to see that even if the cybersecurity law is perfect, it cannot be applied to critical systems operating infrastructure that might be important, but is not regarded as critical infrastructure. On the other hand, it is fair to say that this issue is more common in the EU, as the process to identify critical infrastructure on a national or European level is sometimes ambiguous or obsolete.

Amendment to the legislation has to be expected in case the EU directive on cybersecurity is passed. Despite the fact that the essence of the directive´s draft – communication and cooperation between the public and private sector – is covered by the Czech law, new definitions of market operators have to be incorporated into the law as current definitions of actors will not be sufficient. But this is just a theory until the draft of the directive is finalized and approved.

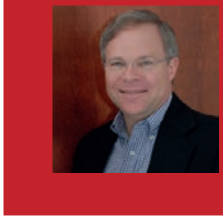
> “ It is the implementation which is the key to actually improving the level of security.

It is possible to conclude that the theoretical apparatus is in place and sufficient. But it is the implementation which is the key to actually improving the level of security. Based on the notices described in this paper, negotiations between the NSA and managers of critical information infrastructure and important networks continue to identify a particular information system, for which the new legal obligations will be valid. Afterwards, a necessary period will be given to the management to actually implement the legal obligations for the selected networks and systems. And only after this implementation is finished, it is possible to say that the level of cybersecurity in the Czech Republic was influenced by the new legislation. This moment in the near future is but only a beginning of a never-ending process to maintain up-to-date standards and measures in order to secure cyberspace. There are many tasks to be performed to actually improve the cybersecurity level in the Czech Republic, and hopefully the NSA together with other stakeholders will manage to do so before Czech cyber assets will become interesting for cyberattackers on a larger level. ■

Bruce Andrews, US Deputy Secretary of Commerce

ANALYSIS

CYBER INNOVATION CENTERS - ACCELERATING THE GROWTH OF CYBER CAPABILITY



JIM JAEGER

Jim Jaeger is the Chief Cyber Strategist at the Fidelis Cybersecurity. As an esteemed security leader, Jim Jaeger is responsible for developing and evolving the company's cyber services strategy and business. In 2015, Rhode Island Governor Gina Raimondo appointed Jim to the state Cyber Commission. Mr. Jaeger has also held leadership roles for a wide range of cyber programs including General Dynamics' support for the DoD Cyber Crime Center (DC3), the Defense Computer Forensic Lab and the DefenseCyber Crime Institute. Mr. Jaeger is a former Brigadier General in the United States Air Force and his military service includes stints as the Director of Intelligence (J2) for the U.S. Atlantic Command, Assistant Deputy Director of Operations at the National Security Agency, and Commander of the Air Force Technical Applications Center.

1. The Role of Cyber Innovation Centers (CIC)

While CICs come in a wide variety of sizes and organizational structures, the common denominator in all CICs is the focus on accelerating the development and evolution of cyber capabilities. Key functions include the development, refinement, and testing of cyber processes and tools. The basic CIC concept is highly flexible and can be easily tailored to serve the unique requirements of the involved organizations.

2.1 Romanian CIC – From Concept to Reality

Romania is employing a two-phased approach to defining and implementing their CIC. This two-phased approach leverages existing security solutions, which include both emerging and potentially competing capabilities. Phase I consists of a structured feasibility study that will provide the foundation for technology prototyping activity in Phase II to further refine stakeholders' requirements in the form of demonstrable cyber capability. The benefit of this approach is that it enables stakeholders to discover emerging technologies while objectively assessing competing technologies from commercial vendors based on technical specifications, cost, and customer requirements. Additionally, this innovation environment will be available for use by the Romanian academic community as well as other invited industrial players to further develop a baseline understanding of cybersecurity technologies' inherent capabilities and limitations.

The inaugural Romanian CIC was established on May 13, 2015 as a joint initiative between the government of Romania of Romania and the United States (US). On that date, senior government officials from both countries cut the ribbon to open the initial pilot CIC, which will serve as the key element in Phase I of the feasibility study for establishing a full-up innovation center. Bruce Andrews, US Deputy Secretary of Commerce, comments on the vital role that CICs play in advancing cybersecurity capability and industry collaboration: "My hope is that we will see more of this kind of collaboration as a result of this Summit – because the most effective way to combat growing threats to our cyberspace is through a strong partnership between industry, government, and civil society. Working together on cybersecurity is a win-win scenario that will make us more resilient to cyberattacks, foster closer ties between our nations and our peoples, create high skill, high wage jobs, and bolster and protect economic prosperity."[1]

2.2 Participants

Several Romanian and US government agencies, along with private-sector organizations representing US industry, are playing key roles in establishing the Romanian CIC. The two primary Romanian organizations leading this initiative are the Ministry of Communications and Information Society and CERT-RO (RO. Centrul National de Raspuns la Incidente de Securitate Cibernetica). The Ministry of Communications and Information Society is the executive agency and provided the facility to house the CIC. The CERT-RO director is dual-hatted as the CIC director and is responsible for the day-to-day operation of the CIC. From the United States, the USTDA (United States Trade and Development Agency) played a central role, with assistance from the US Department of State and the US Department of Commerce. The commercial attachés at the US Embassy generated the initial concept for the Romanian CIC and worked closely with their counterparts in the Romanian government. USTDA sponsored the feasibility study that established the mission and IT architecture of the center. The Department of Commerce also sponsored a US trade mission to Eastern Europe, which highlighted the ribbon cutting for the CIC.[2]

The key industry proponent for the CIC was General Dynamics Fidelis (now Fidelis Cybersecurity).[3] To foster collaboration and facilitate rapid progress, Fidelis cybersecurity personnel leveraged the EDGE Innovation Network approach that General Dynamics has used successfully with various customers, including the US Army's Command Post of the Future program. The extensive cyber experience that the Fidelis team gained over the past 25 years while playing key roles at DC3 (DoD Cyber Crime Center) and the US CERT (US Computer Emergency Response Team) also proved invaluable in developing the plans for the Romanian CIC.

2.3 Romanian CIC Components

Specialized components of the prototype CIC include a training classroom, a test-and-evaluation lab environment, and an agile collaboration room. Supporting infrastructure includes a combined entry and reception area, a lecture hall, and a combined kitchen and break room. The experience gained from deploying this initial capability will contribute directly to refining the requirements and functional design for the follow-on facility. Options include upgrading the prototype facility or developing a completely new, permanent facility.

2.4 Moving Forward

Under the guidance of CERT-RO, the Romanian CIC is now leveraging their prototype facility and resources to partner with other Romanian government and private-industry organizations to explore advanced cyber concepts and organizational relationships; and refine the requirements for the follow-on CIC. Fidelis is now focusing on the planning and documentation to enhance the technical infrastructure of the CIC, and will continue working with the CERT-RO and the Romanian government to enhance the CIC capabilities to meet these evolving requirements.
Romania is committed to partnering with its neighbors to leverage the CIC capabilities across Eastern Europe; however, we recognize that other nations and or-

[1] | Andrews B., Deputy Secretary Bruce Andrews Delivers Keynote Address at Regional Cybersecurity Summit in Bucharest, Romania, 2015 [online] https://www.commerce.gov/news/deputy-secretary-speeches/2015/05/deputy-secretary-bruce-andrews-delivers-keynote-address (access: 13.5.2015).

[2] | USTDA, USTDA Helps Launch Cybersecurity Innovation Center in Romania, 2015 [online] http://www.ustda.gov/news/pressreleases/2015/MENAEE/Romania/PR-Cybersecurity-Innovation-Center-in-Romania_051415/Press-Release-USTDA-Helps-Launch-Cybersecurity-Innovation-Center-in-Romania_051415.asp (access: 14.5.2015).

[3] | Fidelis Cybersecurity, Fidelis Cybersecurity Poised for Next Phase of Growth in Advanced Threat Defense Market, Estimated to Reach Nearly $1 Billion in 2016, 2015 [online] http://www.fidelissecurity.com/fidelis-cybersecurity-poised-next-phase-growth-advanced--threat-defense-market-estimated-reach-nearly (access: 4.5.2015).

ganizations will want to stand up similar facilities. We are seeing interest in CIC capabilities in the Middle East and Asia, as well as Eastern Europe. Fortunately, the CIC approach is very flexible and can be adapted to different national requirements and organizational constructs. In fact, from an innovation standpoint, there is much to be gained by networking CIC-like facilities in different regions. This type of innovation will empower companies not only to successfully combat ever-evolving cyberthreats but also to share and exchange cyber strategies and lessons learned. This is a great first step in globalizing the fight against cybercrime.[4]

2.5 Leveraging the CIC Construct

The CIC construct is recognized as a flexible tool that can be used to crystallize cyber requirements and evolve cyber solutions. Because of its flexible nature, the construct can be tailored to meet the unique needs of other regions and organizations. The name itself also can be tailored to reflect unique regional and organizational influences. For example, while the CIC that the Rhode Island Cyber Commission is considering will have much in common with the Romanian CIC, it will likely be called a CCOE (Cyber Center of Excellence).

> “The CIC construct is recognized as a flexible tool that can be used to crystallize cyber requirements and evolve cyber solutions.

3.1 Funding

There are many different approaches to funding CICs. A $400,175 grant from USTDA along with a cost share by Fidelis funded the feasibility study of the CIC. The Romanian CIC was established based upon the results of the study by the Romanian government which provided the facility, basic infrastructure, and equipment. Fidelis provided a range of services, including cyber training, planning and project management, and licenses for key cyber software systems. Alternatively, a similar CIC in Bossier City, Louisiana was initially funded by state and local governments.[5]

3.2 Functions

Because the CIC construct is inherently flexible, the functions of each CIC should be tailored to meet the unique requirements of the sponsoring organizations. These functions typically include training, evaluation of new cyber concepts, technology testing, and information sharing.

3.3 Training and Education

The demand for the cyber skills needed to counter today's advanced attacks far outpaces the availability of trained and experienced cyber personnel. Training and education facilities are therefore a cornerstone of most CICs. Some of the most critically needed skills are in network incident response and live network forensics. Malware reverse engineering skills are also in short supply. These are hands-on skills that cannot typically be taught in a conventional classroom. Cyber labs with live network simulations are thus required to turn classroom knowledge into “in-the-trenches” skills and expertise.

3.4 Collaboration and Information Sharing

Many of the sophisticated cyberattacks that we see today can only be countered through coordinated responses involving multiple internal staff functions as well as external organizations. Recent successes against cybercriminals often involve multiple nations sharing data and coordinating their response actions. As a result, CICs typically include secure collaborative conferencing systems supported by analytic tools.

3.5 Simulation and Evaluation

The requirement to bring together government and industry personnel to explore new cyberdefence concepts and strategies often drives the need for simulation environments to evaluate those approaches. Typically, these simulation environments build on the tools used for cyber training, but require higher fidelity and flexibility to support testing and evaluation

[4] | Jaeger, J., Enhancing Cybersecurity in Eastern Europe, 2015 [online] http://www.threatgeek.com/2015/05/enhancing-cybersecurity-in-eastern-europe.html#more (access: 27.5.2015).

[5] | Prime J A., CIC Fills First Phase, Eyes Future, 2015 [online] http://www.cyberinnovationcenter.org/cic-fills-first-phase-eyes-future/ (access: 26.5.2015).

of new cyber strategies, processes, and organizational constructs. Fortunately, a wide range of simulations based on the needs of the involved organizations are available.

> “The requirement to bring together government and industry personnel to explore new cyberdefence concepts and strategies often drives the need for simulation environments to evaluate those approaches.

3.6 Typical Participants

The Romanian CIC includes both government and industry participants. While Fidelis Cybersecurity is playing a central role in Romania, it is anticipated that other industry partners will join the effort in the near future and will contribute cybersecurity tools to enhance the training and testing infrastructures. In many environments, universities are likely to be key participants as well. The Indonesian CIC, which is in its early planning stages, will likely include the Indonesian National Defence University as a primary participant. Similarly, the Rhode Island Cyber COE, which is under discussion, is likely to include a key role for the Naval War College in Newport, Rhode Island.

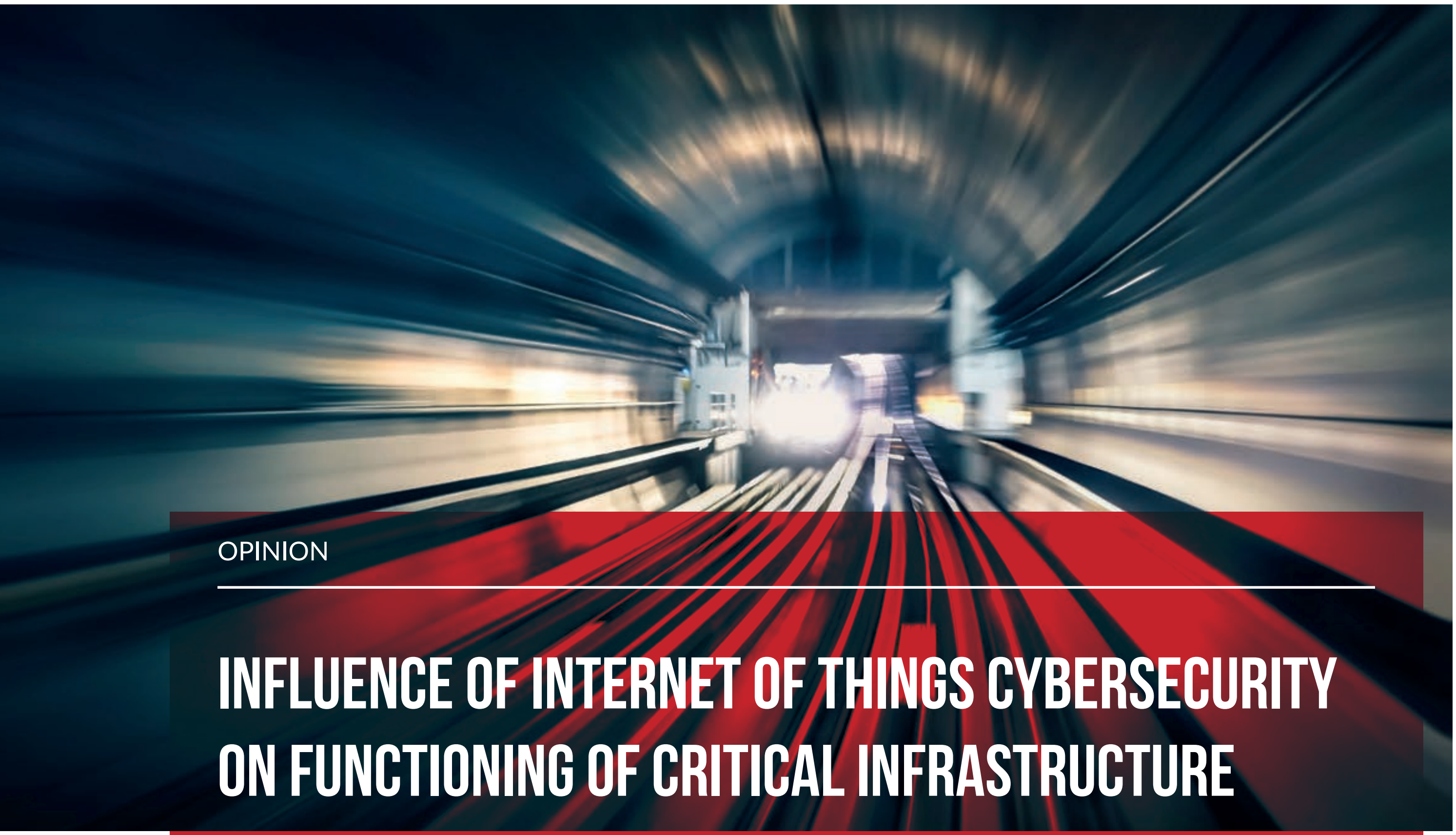
Conclusion

To successfully secure the modern enterprise against advanced threats it is vital that organizations build strong relationships between the team of security experts, the cybersecurity processes, and the technologies employed to defend the networks. Effective cybersecurity begins by understanding the methods and techniques used by advanced adversaries. Organizations can then strengthen their cyberdefences and more effectively manage targeted attacks by leveraging the vast experience of the cybersecurity community. CICs provide the critical organizational construct to focus and accelerate these efforts.

The Romanian CIC illustrates how government and industry can effectively work together to advance cybersecurity capabilities. The Romanian and US partnership overcame the challenges associated with securing the appropriate team, processes, and technologies by tailoring the CIC to Romania’s unique needs and requirements. Furthermore, it focused the rapidly growing Romanian cyber community on interaction and analysis to develop operational requirements that drive procurement decisions. The CIC’s open framework is enabling impartial technical analysis of alternatives, thereby allowing stakeholders to make the most informed decisions prior to technology acquisitions. The project success and resulting innovation will empower organizations to combat ever-evolving cyber threats and to share cyber strategies and lessons learned.

At Fidelis, we look forward to helping organizations to assess their security posture accurately and objectively; identify the requirements necessary to design, build, and manage a CIC; provide a cybersecurity framework that can assess technologies to prevent, discover, investigate, and contain advanced threats; and empower stakeholders to respond to sophisticated attacks quickly and effectively with the most mature solutions and CONOPs (Concept of Operations). ■

The exchange of experience
in the area of cybersecurity is treated as
a necessity in PERN „Przyjaźń" S.A.
www.pern.com.pl
PERN „Przyjaźń" S.A.



OPINION

INFLUENCE OF INTERNET OF THINGS CYBERSECURITY ON FUNCTIONING OF CRITICAL INFRASTRUCTURE

ANDRZEJ TYMECKI

Andrzej Tymecki is an expert on new telecommunications techniques, for 20 years associated with the telecommunications industry. Author of Polish and international publications on fibre optics. Since 1998, he has been a member of IEC and CENELEC standardisation committees, representing Poland. Previously working at Orange Polska and France Telecom Group and since 2014, he is a Vice President of the Board of Exatel SA, in the field of technology.

The article was written in cooperation with Tomasz Łużak – Solutions Manager and Artur Świacki – ICT Expert from Exatel.

Experts from the IT industry predict that it will not be long before all the devices that surround us every day, starting from washing machines, refrigerators, or cars and ending with systems ensuring the power supply – will be communicating with each other via the Internet. The concept that assumes such a model of synergy of devices is called the Internet of Things (IoT). In the opinion of suppliers of network security solutions and IT solutions, as well as leading consulting companies, by the year 2020, 50 billion devices will be connected to the network. In connection with such massive development of the IoT, it seems justified to ask questions about both the benefits and risks stemming from the new model of life in the environment of advanced technologies.

Articles on professional websites and reports of research companies devoted to the IoT indicate the possibility of enjoying benefits from the development of this technology in many areas of life. The point is made that the consequence of the development of the IoT will be, among other things, economic growth, an increase in the number of new jobs, improvement of the healthcare system, as well as the field of security:

"With the help of cameras and sensors, there is the possibility to guard against, or avoid, physical threats, which might occur at the workplace or home. In time, even disaster management or recovery systems will get help from IoT".[1]

[1] | EY Cybersecurity and the Internet of Things, March 2015, p. 4.

Unfortunately, there is also the other side of the IoT, e.g. taking over control of vehicles via the Internet, which so far could have been seen only in some movies and is presently becoming possible in the world of the Internet of Things. A well-known security researcher, Charlie Miller made it clear in a very impressive manner, when he took control of the car of a journalist who agreed to take part in that blood chilling experiment via the Internet. The results of the experiment were surprising: the hacker controlled the operation of the brakes of the car, the gear box, the radio receiver, the air conditioning system, and the wipers. Unfortunately, the test also demonstrated that the hacker was able to control the steering wheel of the car.[2]

Now, how do the positive forecasts for the development of security in the world of IoT relate to the results of the experiment described above?

Well, practically any device connected to the network (via a mobile application or a website) may become the object of an attack by a cybercriminal, if it is not properly protected. Not so long ago, specialist internet websites wrote at length about internet-controlled attacks on Japanese toilets[3] or bulbs[4]. And though the previous example of taking over control of a car seems to be a more serious situation than the sudden lack of electricity at our homes or going out of the toilet with your suit completely wet, all these stories show us what consequences we may face in connection with too light of an approach to security issues in the world of the IoT. Here, the situation is varied.

In 2014, the HP company tested 10 popular devices connected to the Internet in terms of security. The results of the test can be considered alarming. It was concluded that 70% of them contained security exposures, 80% of them did not require passwords of sufficient complexity of length, 90% collected at least one piece of personal information, and 70% allowed the attacker to identify a valid account through account enumeration.[5]

> “In 2014, the HP company tested 10 popular devices connected to the Internet in terms of security. The results of the test can be considered alarming.

It is worth remembering that we all share the responsibility for implementation of necessary protective measures. However, there is one area in the case of which this responsibility rests for the most part with the state, and the consequence of not giving too serious consideration to the problem by the authorities may be severe for each citizen. The whole issue is about the security of critical infrastructure which comprises, among other things, the energy production systems at power plants, air traffic control systems, transmission networks, or national defence systems.

A large portion of the elements of critical infrastructure is based on the SCADA IT system (Supervisory Control And Data Acquisition), which supervises the course of the technological or production process. Its main functions cover data (measurements) collection, their visualisation, process control, alarms, and data archiving.

The report of the Symantec company „Description of Security Gaps in the SCADA System” indicates improper system protection, and the mistaken perception of this system by the decision-making persons in public utility companies is seen as the source of the problems related to this. In the opinion of the Symantec experts, this makes the implementation of the best strategies for IT protections impossible.

Firstly, the experts claim that IT managers in public utility companies share a mistaken belief that since the majority of SCADA systems was created before other

[2] 2 Greenberg A., Hackers remotely kill a Jeep on the highway – with men in it, 2015 [online] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (access: 04.09.2015).

[3] Kooser A., High-tech toilet gets hacker warning; nothing is safe.[online] http://www.cnet.com/news/high-tech-toilet-gets-hacker-warning-nothing-is-safe/ (access: 04.09.2015).

[4] Crist R., Hackers find security weaknesses with the Lifx smart LED., [online] http://www.cnet.com/news/hackers-discover-security-weaknesses-within-the-lifx-smart-led/(access: 04.09.2015).

[5] McAfee Labs, Threats Predictions, 2015.

corporate networks, it is not possible to gain access to them neither through corporate networks nor from other access points. Such a thesis is mistaken, as there is often a physical connection between SCADA networks and corporate IT systems. At the same time, the basic IT infrastructure protection strategies at public utility companies often ignore the fact that gaining access to the corporate network makes gaining unauthorised access and taking over control of the SCADA system possible.

Secondly, in the opinion of the Symantec experts, only few public utility companies protect all the access points to the SCADA network properly, despite the recommendations regarding the necessity of using internal firewalls and intrusion detection systems (IDS) between corporate networks and SCADA systems.

> “ The belief of the public utility companies' IT management that gaining unauthorised access to the SCADA system by cybercriminals is difficult is indicated as the third cause of the weakness of the SCADA system by the experts.

The belief of the public utility companies' IT management that gaining unauthorised access to the SCADA system by cybercriminals is difficult is indicated as the third cause of the weakness of the SCADA system by the experts. According to the said experts, this belief is based on another mistaken assumption, namely, that no person who attacks a given SCADA system can gain information on how it was designed and implemented. The experts from Symantec point to the fact that public utility companies, if only for the fact of their importance, constitute more than a probable target of attacks of cybercriminals. The experts emphasise that a well prepared group of cybercriminals, whose aim is to cut off supplies to public utility companies will not hesitate to gain detailed information about the SCADA systems and possible security gaps. The risk is additionally increased by the increasing availability of information on how the SCADA systems operate.[6] It is worth knowing that through the appliances which will create the Internet of Things, such as refrigerators or washing machines, it will be possible to get to the contact points with the production systems such as SCADA – on which a large portion of critical infrastructure elements is based – and to carry out an attack that will seriously threaten the state's security. It is also worth asking a question, how the critical infrastructure would operate, if, all of a sudden, we found ourselves facing a serious external threat? Taking into account the degree of connection with the critical infrastructure systems, which the IoT will shortly achieve, the contribution of the government to ensuring its cybersecurity seems to be indispensable. Just as one of the most essential human needs is the need for security, the most important task of each state is the permanent improvement of its security systems. ■

[6] | Symantec, Opis luk w zabezpieczeniach systemu SCADA, p. 4-5.

EUROPEAN CYBERSECURITY FORUM

Annual Public Policy Conference dedicated to strategic aspects of cybersecurity

AUTUMN 2016

CYBERSEC 2016

STAY TUNED

WWW.CYBERSECFORUM.EU

EUROPEAN CYBERSECURITY JOURNAL

SUBSCRIPTION AND ORDERING INFORMATION

EUROPEAN CYBERSECURITY JOURNAL
STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES
ANALYSES • POLICY REVIEWS • OPINIONS
The Kosciuszko Institute

Subscribe now and stay up to date with the latest trends, recommendations and regulations in the area of cybersecurity. Unique European perspective, objectivity, real passion and comprehensive overview of the topic – thanks to these features, the European Cybersecurity Journal will provide you with an outstanding reading experience, from cover to cover.

The ECJ is addressed to leaders and decision makers from both private and public sector professionally related to the topic of cybersecurity, as well as to other cybersecurity stakeholders. The quarterly brings together top-level managers, governmental and military officials, European-level representatives and academics. Acknowledging the fact that cybersecurity should be discussed globally, authors and readers of the ECJ shape a holistic, multidimensional network.

THE ECJ IS ADRESSED TO

- CEOs, CIOs, CSOs, CISOs, CTOs, CROs
- IT/Security Vice Presidents, Directors, Managers
- Legal Professionals
- Governance, Audit, Risk, Compliance Managers & Consultants
- Government and Regulatory Affairs Directors & Managers
- National and Local Government Officials
- Law Enforcement & Intelligence Officers
- Millitary & MoD Officials
- Internat. Organisations Reps.

FROM THE FOLLOWING SECTORS

- ICT
- Power Generation & Distribution
- Transportation
- Critical Infrastructure
- Defence & Security
- Finance & insurance
- Chemical Industries
- Mining & Petroleum
- Public Utilities
- Data Privacy
- Cybersecurity
- Manufacturing & Automotive
- Pharmaceutical

PRICING OF THE ANNUAL SUBSCRIPTION (4 ISSUES: 2/2015 - 2/2016)

Hard copy: €199
excluding VAT, including postage and handling

Electronic edition: €199
excluding VAT, including handling

Hard copy and electronic edition: €249
excluding VAT, including postage and handling

ORDERING INFORMATION

In order to subscribe, please send an inquiry to the publisher. Detailed terms of sale and delivery information are available upon request.

The Kosciuszko Institute
editor@cybersecforum.eu
ul. Lenartowicza 7/4
31-138 Kraków, Poland
Tel: +48.12.632.97.24

The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship project in the field of cybersecurity, within which the CYBERSEC Forum is organized.

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN
CYBERSECURITY JOURNAL